Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu de travail

Robert, Romain; Rosier, Karen

Published in:
Le droit du travail à l'ère du numérique

Publication date:
2011

Document Version
le PDF de l'éditeur

Réglementation et contrôle de l'utilisation des technologies de la communication et de l'information sur le lieu du travail

Romain Robert

Avocat au barreau de Bruxelles
Chercheur au Centre de Recherche Information, Droit et Société (CRIDS) – F.U.N.D.P.

Karen Rosier

Avocate au barreau de Namur
Chercheuse au Centre de Recherche Information, Droit et Société (CRIDS) – F.U.N.D.P.
Assistante à la Faculté de droit des F.U.N.D.P.

Chapitre 1
Vie privée du travailleur sur le lieu du travail : concilier… l'inconciliable ?

1. Le droit du travailleur au respect de sa vie privée sur le lieu de travail est aujourd'hui incontesté. Tout juste entend-t-on des voix s'élever pour rappeler que ce droit n'est cependant pas absolu. Et c'est précisément la question de la délimitation de ce qui peut être admis comme ingérence dans la vie privée du travailleur qui se pose avec une acuité évidente dans le monde du travail.

En effet, une caractéristique essentielle du contrat de travail est le lien de subordination. Celui-ci implique que l'employeur puisse donner des instructions au travailleur et exercer une autorité sur celui-ci. La nécessaire conciliation entre ces prérogatives de l'employeur et le droit du travailleur au respect de sa vie privée nous amène à nous poser deux questions cruciales.

La première consiste à se demander quelle est la marge de manœuvre de l'employeur dans la réglementation de l'utilisation des outils de communications électroniques au sein de son entreprise : l'employeur peut-il interdire tout usage non professionnel de cet outil ?

La seconde a trait à la délicate question de la cohabitation entre l'autorité de l'employeur et le respect de la vie privée dû au travailleur. En effet, qu'en est-il de l'effectivité de l'autorité de l'employeur s'il ne lui est pas permis de vérifier que ses instructions sont bien suivies d'effet, en ayant accès aux communications réalisées par ses travailleurs ? D'un autre côté, l'introduction de nouveaux modes de communication n'induit-il pas également une nécessaire redéfinition de ce qui relève de protection de la vie privée : on ne communique pas par courrier électronique comme on le fait par courrier papier.

2. Nous le verrons, les dispositions qui participent de la protection de la vie privée du travailleur empêchent en réalité bon nombre de mesures de contrôle sur l'usage que le travailleur fait de l'outil de communication électronique mis à sa disposition par l'employeur.

Le terme de « contrôle » peut, à notre sens, recouvrir deux réalités bien différentes. Il peut intervenir *a priori*, dans la définition de règles à respecter concernant l'usage de l'outil de communication électronique. Il peut, par ailleurs, intervenir *a posteriori* et prendre ainsi la forme d'une vérification de l'usage qui a été fait de l'outil de communication. À cet égard, il y a lieu de remarquer qu'il ne s'agit pas uniquement de vérifier que le travailleur a bien respecté les consignes qui lui ont éventuellement été données par l'employeur sur l'usage de cet outil. Bien souvent, ce contrôle se traduit par une prise de connaissance de certains messages envoyés par e-mail ou par SMS ou de sites internet consultés pour établir l'existence d'un comportement problématique qui pourrait, le cas échéant, justifier le licenciement du travailleur pour motif grave.

Préalablement à l'examen de ces deux facettes de la problématique du contrôle, nous nous proposons de faire le point sur le cadre légal dans lequel elles s'inscrivent.

Chapitre 2
Panorama des dispositions applicables

Section 1
Quelques balises

3. La réglementation en la matière est multiple. Multiple, tout d'abord, car plus d'un texte est d'application. Multiple, ensuite, car toutes les dispositions ne vont pas nécessairement dans le même sens. Un état des lieux s'impose avant de pouvoir tirer les conclusions qui résultent de l'application cumulative des dispositions pertinentes.

L'objet du présent chapitre est donc d'identifier quelles règles sont applicables lorsqu'il s'agit de contrôler le travailleur dans l'utilisation qu'il fait de son outil de travail (e-mail, internet, téléphone) ou par le biais d'une technologie de communication (contrôle via la géolocalisation).

Nous envisagerons également dans quelle mesure l'employeur peut interdire l'enregistrement de fichiers personnels sur l'ordinateur d'un travailleur ou avoir accès aux fichiers qui y sont stockés.

Il convient de remarquer d'emblée que les particularités de la relation de travail n'ont pas été prises en compte par le législateur. Ceci explique sans doute que les partenaires sociaux se soient employés à tenter de définir comment il conviendrait d'aborder la législation existante dans le contexte de la relation de travail. Nous y reviendrons dans le cadre de l'analyse de la convention collective de travail n° 81[1].

Section 2
Autorité de d'employeur *versus* vie privée

A. Les fondements du pouvoir de contrôle de l'employeur

1. Loi du 3 juillet 1978

4. Le lien de subordination relève de l'essence même du contrat de travail[2]. Aussi, l'employeur dispose-t-il d'un pouvoir de contrôle sur les travailleurs. Comme le relève la doctrine, il paraît évident qu'un employeur doit pouvoir vérifier si le travail est effectué correctement et si les instructions données par l'employeur sont respectées[3]. Les dispositions de la loi du 3 juillet 1978 relatives au contrat de travail qui sont généralement citées comme fondement légal à un pouvoir de surveillance ou de contrôle sont les articles 16 et 17 qui imposent aux travailleurs certaines obligations. Le pouvoir de contrôle de l'employeur n'est donc pas affirmé tel quel dans le loi mais se trouve être le corollaire nécessaire des obligations mises à charge du travailleur : obligation de respecter leur employeur ainsi que les convenances et les bonnes mœurs, d'exécuter leur travail avec soin, probité et conscience, au temps, au lieu et dans les conditions convenus ou encore d'agir conformément aux ordres et aux ins-

---

1 C.C.T. du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication en réseau, rendue obligatoire par l'A.R. du 21 juin 2002 (*M.B.*, 29 juin 2002).

2 *Cf.* notamment Art. 2 et 3 de la loi du 3 juillet 1978 relative au contrat de travail.

3 S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. du Jeune Barreau de Bruxelles, 2005, p. 142.

tructions qui lui sont donnés par l'employeur, ses mandataires ou ses préposés, en vue de l'exécution du contrat.

5. En outre, puisque l'employeur doit mettre à disposition du travailleur les technologies nécessaires à l'accomplissement du travail[4], il semble approprié que le corollaire de cette obligation constitue la possibilité pour l'employeur de définir l'utilisation qui peut en être faite.

Il en découle que, dans le respect des dispositions légales, réglementaires et contractuelles, l'employeur est libre de déterminer les conditions d'exécution du contrat de travail, comme par exemple les modalités d'utilisation des technologies mises à disposition du travailleur sous la responsabilité de l'employeur[5].

La Cour du travail de Gand a ainsi estimé que « l'employeur a le droit, en vertu de la loi relative aux contrats de travail, d'instaurer unilatéralement des directives et obligations quant à l'informatique sans consensus ou implications des travailleurs »[6].

La C.C.T. nº 81 stipule d'ailleurs en son article 3 que « les travailleurs reconnaissent le principe selon lequel l'employeur dispose d'un droit de contrôle sur l'outil de travail et sur l'utilisation de cet outil par le travailleur dans le cadre de l'exécution de ses obligations contractuelles, y compris lorsque cette utilisation relève de la sphère privée, compte tenu des modalités d'application prévues par la présente convention ».

6. Ce pouvoir paraît encore renforcé par les principes applicables en matière de responsabilité de l'employeur pour les actes posés par les employés[7]. L'em-

---

4 En vertu de l'article 20 de la loi du 3 juillet 1978 sur les contrats de travail, l'employeur a l'obligation de faire travailler le travailleur dans les conditions, au temps et au lieu convenus, notamment en mettant à sa disposition, s'il y échet et sauf stipulation contraire, l'aide, les instruments et les matières nécessaires à l'accomplissement du travail.

5 O. Rijckaert, « La protection de la vie privée du travailleur : principes et cadre juridique », *in Surveillance électronique et travailleurs et usage des TIC à des fins privées sur le lieu de travail*, FEB, 2002, p. 25 ; S. van Wassenhove, M. De Leersnyder, G. Chuffart, *Nouvelles Technologies et leur impact sur le droit du travail*, Bruxelles, Heule, 2003, p. 38 ; H. Barth, « Contrôle de l'employeur de l'utilisation « privée » que font ses travailleurs des nouvelles technologies de l'information et de communication au lieu de travail », *J.T.T.*, 2002, p. 171 ; R. Blanpain et M. van Gestel, *Use and monitoring of Email, Intranet and internet Facilities at Work*, La Haye, Kluwer International, 2004, p. 168 ; voyez également en ce sens : Commission de la protection de la vie privée, Avis nº 39/2001 concernant la proposition de loi 2-891/1 du 29 août 2001 visant à réglementer l'utilisation des moyens de télécommunication sur le lieu de travail, du 8 octobre 2001, p. 5, www.privacycommission.be.

6 C. trav. Gand, 4 avril 2001, *J.T.T.*, 2002, p. 49 ; nous verrons que cette conclusion de la Cour doit être nuancée dès lors qu'une consultation sociale est désormais notamment prévue par la C.C.T. nº 81 lors de l'élaboration d'une réglementation de l'usage des technologies.

7 *Cf.* Art. 18 de la loi du 3 juillet 1978 relative au contrat de travail et art. 1384, §§ 1 et 3 du Code civil. Nous vous renvoyons également sur cette question à la contribution de Romain Marchetti qui y est consacrée dans le présent ouvrage.

ployeur aura tout intérêt à réglementer ou limiter l'utilisation qui pourra être faite de son matériel dès lors qu'il devra le plus souvent supporter la responsabilité des abus qui découlerait de l'abus ou de l'usage inadéquat des moyens informatiques mis à sa disposition[8].

Si le principe du pouvoir de contrôle ne souffre aucune discussion, il demeure que l'on peut s'interroger sur l'étendue des prérogatives qui en découlent. En effet, en vertu de la relation de travail-même, le travailleur renonce à une partie de sa liberté, sur laquelle l'employeur pourra exercer son pouvoir d'autorité. Même s'il convient de distinguer le travailleur des prestations qu'il fournit, il est certain que contrôler ces prestations reviendra à contrôler en partie le travailleur lui-même[9]. Toutefois, se mettre à la disposition d'un employeur en vertu d'un contrat de travail ne signifie pas pour autant que l'on renonce à ses droits constitutionnels[10].

Sur ce point, il nous faut constater que les opinions des auteurs de doctrine divergent. Comme nous le verrons ci-après, diverses dispositions ayant trait au droit au respect de la vie privée et au secret des communications électroniques font obstacle à une prise de connaissance des e-mails de ce dernier, la surveillance de ses connexions à l'internet, le contrôle de l'utilisation fait de son GSM professionnel, etc. Des ingérences sont toutefois possibles si elles sont prévues par une « loi ». La question se pose dès lors de savoir si les articles 16 et/ou 17 peuvent constituer des bases légales suffisantes pour justifier de telles ingérences dans la vie privée du travailleur et, sur ce point, il n'y a pas d'unanimité en doctrine ni en jurisprudence[11].

2. Article 544 du Code civil

7. En application de l'article 544 du Code civil, il est admis qu'en tant que propriétaire de l'outil mis à la disposition du travailleur, l'employeur ait le droit

---

8 S. van Wassenhove, M. De Leersnyder, G. Chuffart, *Nouvelles Technologies et leur impact sur le droit du travail*, Heule, Bruxelles, 2003, pp. 34 et 109 à 124 ; Th. Claeys et D. Dejonghe, « Gebruik van *e-mail* en internet op de werkplaats en de controle door de werkgevers », *J.T.T.*, 2001, p. 134.

9 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 32-33, n° 65. C'est d'ailleurs en invoquant le droit de contrôle consacré par l'article 17, 2° de la loi sur le contrat de travail que le Tribunal du travail de Bruxelles a accepté que l'employeur produise un e-mail dont le contenu était pornographique envoyé par un travailleur à un collègue (Trib trav. Bruxelles, 22 juin 2000, *Computerrecht*, 2001, p. 311). Selon le Tribunal, l'employé ne pouvait abuser de son droit à la vie privée pour s'opposer au dépôt des éléments de preuve ainsi récoltés. Le Tribunal du travail de Bruxelles a également considéré à cet égard que « les restrictions qui s'opposent à un usage absolu de l'exercice du droit à la vie privée dans le cadre des relations de travail découlent, fût-ce indirectement, de la loi du juillet 1978 relative aux contrats de travail, et plus précisément des articles 16 et 17 de ladite loi décrivant les obligations réciproques des parties » (Trib trav. Bruxelles, 16 septembre 2004, *J.T.T.*, 2005, p. 61).

10 P. Humblet, « Het grondrecht op privacy : een blinde vlek in het arbeidsrecht », *in Tegenspraak. Cahier 14. Mensenrechten. Tussen retoriek en realiteit,* Gent, Mys and Breesch, 1994, pp. 215-216.

11 Nous y reviendrons sous le section 3, B du présent chapitre.

de déterminer les conditions dans lesquelles l'outil informatique et, de manière plus large, l'utilisation du réseau, peut être fait[12].

Aussi F. Hendrickx rappelle-t-il que l'employeur doit être considéré comme le propriétaire d'un moyen de production et qu'à ce titre, il peut parfaitement décider d'interdire à des tiers, qu'ils soient employés, ou tiers à l'entreprise d'en faire usage ; cela vaut aussi bien pour le téléphone que pour la photocopieuse[13].

Nous verrons toutefois que le droit de règlementer l'usage des outils de communication électronique, fondé sur le droit de propriété de l'employeur, ne lui donne pas un droit absolu de contrôle au prétexte que le matériel en question lui appartient. L'exercice de ce droit peut se voir ainsi limité par le droit au respect de la vie privée[14]. C'est ce que rappelle le Tribunal de travail de Bruxelles dans un jugement du 2 mai 2002 : « Il pourrait être soutenu que l'employé a utilisé le matériel dans un but qui n'était pas celui pour lequel il a été confié, ce qui pourrait constituer une atteinte au droit de l'employeur. Cette atteinte n'a pas pour effet de supprimer la protection de la vie privée, il s'agit de concilier deux droits contradictoires […] » [15].

B. Le droit au respect de la vie privée : un principe fondamental

8. Les articles 8 de la C.E.D.H. et 22 de la Constitution consacrent le droit au respect de la vie privée.

1. L'article 8 de la C.E.D.H.

a. Objet de la protection

9. La jurisprudence de la Cour européenne des droits de l'homme a clairement établi que le travailleur jouit également de cette protection sur le lieu

---

12 Pour la jurisprudence s'appuyant sur cette disposition, voyez celle citée dans : S. van Wassenhove, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. du Jeune Barreau de Bruxelles, 2005, p. 143 ; voyez également en ce sens : S. van Wassenhove, M. de Leersnyder, G. Chuffart, *Nouvelles Technologies et leur impact sur le droit du travail*, Heule, Bruxelles, 2003, p. 143.

13 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 183.

14 S. van Wassenhove, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. du Jeune Barreau de Bruxelles, 2005, p. 144.

15 Trib. trav. Bruxelles (24e ch.), 2 mai 2000, R.G. nº 00/08438, www.droit-technologie.org.

de travail[16]. Nous épinglerons en particulier l'arrêt *Copland* du 3 avril 2007[17] dans lequel la Cour Européenne des droits de l'homme a déclaré fondée la plainte portée par une employée d'une école privée britannique contre son employeur en raison de la surveillance systématique de l'emploi d'internet, des e-mails et du téléphone par ce dernier. La Cour examina si, en l'espèce, on pouvait effectivement parler d'atteinte à la « vie privée » à propos de l'usage des moyens de communication sur son lieu de travail. Elle considéra que tel était le cas en l'espèce dès lors que l'employée n'avait pas été informée de possibles contrôles et pouvait donc légitimement supposer que l'usage qu'elle faisait du téléphone, de l'internet et du courrier électronique était protégés par le respect dû à sa vie privée.

b. Effet direct et horizontal de la disposition

10. L'article 8 de la C.E.D.H. a, en droit belge, un effet direct ou vertical : ceci implique que les citoyens peuvent directement s'en prévaloir. Par ailleurs, cette disposition initialement prévue pour assurer la protection du citoyen contre les agissements des autorités publiques reçoit en droit belge un champ d'application *horizontal*[18]. Comme le résume la Cour du travail de Mons dans un arrêt du 22 mai 2007, « Il est admis par la doctrine et la jurisprudence que l'article 8 de la Convention européenne des droits de l'homme est également applicable aux personnes privées, lesquelles ne peuvent s'ingérer dans la vie privée d'autrui que dans le respect des conditions requises dans le chef des autorités publiques »[19]. Cette solution implique donc que l'employeur est tenu au respect de l'article 8 de la C.E.D.H. dans ses relations avec les travailleurs[20].

On constate que certaines décisions de jurisprudence rendues en matière de contrôle *a posteriori* de l'usage des outils de communications électroniques se

---

16 Cour eur. D.H., arrêt *Niemietz c. Allemagne*, 16 décembre 1992, Série A., n° 251 ; Cour eur. D.H., arrêt *Halford c. Royaume-Uni*, 25 juin 1997, Rec. 1997 – III, 39 ; Cour eur. D.H., arrêt *Kopp c. Suisse* du 24 mars 1998, Rec. 1998-II, p. 540, § 53 ; Cour eur. D.H., arrêt *Amann c. Suisse*, 16 février 2000, *Publ. Cour eur. D.H.*, 2000-II, p. 244, § 65.

17 Cour eur. D.H., arrêt *Copland c. Royaume-Uni*, 3 avril 2007, Requête n° 62617/00, http://www.echr.coe.int/echr/.

18 J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-F. Leclerq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, p. 38 ; J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, p. 82 et réf. citées.

19 C. trav. Mons, 22 mai 2007, *J.T.T.*, 2008, p. 177 ; *R.D.T.I.*, 2008, p. 228, obs. K. Rosier et S. Gilson.

20 Trib. trav. Bruxelles (24e ch.), 2 mai 2000, R.G. n° 00/08438, www.droit-technologie.org ; Trib. trav. Hasselt (1re ch.), 21 octobre 2002, R.G. n° 2020348, www.cass.be ; C. trav. Anvers, 15 décembre 2004 ; R.G. nos 2004-0295, www.cass.be.

bornent d'ailleurs à constater une violation de l'article 8 de la C.E.D.H. pour sanctionner le comportement d'un employeur par trop intrusif[21].

c. Limites du droit au respect de la vie privée

11. Concrètement, l'application de l'article 8 de la C.E.D.H. implique que sont seules admises les atteintes à la vie privée qui répondent à certaines conditions. En effet, l'article 8, al. 2 de la Convention dispose que :

> « 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 ».

§ 1er Le principe de légalité

12. L'ingérence doit tout d'abord être prévue par une « loi » qui soit suffisamment précise, claire, accessible et prévisible[22]. Cette exigence traduit le *principe de légalité*. Pour l'application dudit article 8, le terme « loi » désigne toute norme de droit interne, écrite ou non, pour autant que celle-ci soit accessible aux personnes concernées et soit énoncée de manière précise[23]. S'est ainsi posée la question de savoir si l'article 17, 1° et 2° de la loi sur les contrats de travail était susceptible de constituer une base légale suffisante résistant à l'exigence de légalité susmentionnée pour ce qui est du contrôle des e-mail. La doctrine et la jurisprudence restent divisées à ce sujet[24]. Nous pensons qu'il convient de répondre par la négative à cette question dès lors que la norme ne rencontrera pas le degré de prévisibilité requis[25]. L'arrêt *Copland* rendu par la Cour européenne des droits de l'homme nous conforte dans cette opinion[26]. Dans cet arrêt évoqué ci-avant et rendu dans le cadre d'un litige portant sur le contrôle des e-mails et de l'usage de l'internet par un travailleuse, la Cour eut

---

21 C. trav. Bruxelles (4e ch.), 3 mai 2006, R.G. nº 45.922, www.cass.be.

22 Voy. notamment : Cour eur. D. H., Arrêt *Sunday Times*, 26 avril 1979, Série A, nº 30, § 49.

23 Cass., 2 mai 1990, *J.T.*, 1990, p. 469.

24 Dans le sens d'un pouvoir d'ingérence inhérent à la relation de travail : R. de Corte, « Surfen op het werk : een kwestie van niet uitglijden », *De juristenkrant*, 7 novembre 2000, p. 7 ; F. Lagasse, « La vie privée et le droit du travail », *Chron. D. S.*, 1997, p. 425 ; dans un sens inverse : voy. note S. van Wassenhove, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. du Jeune Barreau de Bruxelles, 2005, p. 143 ; O. Moreno et S. Van Koekenbeek, « Les mutations de la vie privée au travail », *Orientations*, n°35, 2005, p. 17.

25 Voy. F Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 61. Pour M. Hendrickx, l'article 17 de la loi sur les contrats de travail ne peut offrir une base suffisante à des atteintes à la vie privée qu'en ce qui concerne l'exercice normal de l'autorité patronale.

26 Cour eur. D.H., arrêt *Copland c. Royaume-Uni*, 3 avril 2007, Requête nº 62617/00, http://www.echr.coe.int/echr/.

à vérifier dans quelle mesure l'établissement scolaire qui l'employait était fondé à invoquer l'existence d'un pouvoir octroyé par la loi l'autorisant à prendre toute mesure nécessaire ou opportune à ses activités pour justifier la violation de la vie privée constatée par la Cour. La Cour a précisé qu'aux termes de la jurisprudence en la matière, il est exigé que la loi en question énonce de façon suffisamment claire les circonstances et conditions dans lesquelles l'autorité publique est à même de prendre des mesures susceptibles de porter atteinte à la vie privée des personnes concernées, ce qui n'est pas le cas en l'espèce.

Il nous apparaît que la loi du 3 juillet 1978 n'est pas suffisamment précise que pour justifier des contrôles concernant l'utilisation des outils de communications électroniques et ne répond pas à l'exigence de prévisibilité.

13. Ceci étant, au regard de l'article 8 de la C.ED.H., la norme requise ne doit donc pas nécessairement être une loi au sens formel du terme mais peut parfaitement consister en une norme privée[27], tel par exemple un règlement de travail[28], le contrat de travail, une charte d'utilisation de l'e-mail et de l'internet. Comme le pointe H. Barth, « il suffit que l'ingérence soit prévue dans une règle claire et précise accessible au travailleur, de façon qu'il puisse prévoir les suites et adapter son comportement de travail ou même une fiche d'instruction peut déjà satisfaire à cette condition »[29].

Ces principes prennent toute leur importance lorsqu'il s'agit de déterminer l'instrument de régulation le plus approprié pour définir les modalités d'un contrôle envisagé sur le lieu de travail. L'exigence de légalité posée par l'article 8 C.E.D.H. nous semble donc rencontrée lorsque l'existence et les modalités du contrôle des moyens de communications sont décrites dans un document suffisamment accessible et prévisible établi par l'employeur, concernant les contrôles qui seront exercés sur les moyens informatiques utilisés.

Une des manières d'assurer cette transparence est d'obtenir le consentement de la personne concernée par de possibles ingérences dans sa vie privée.

---

27 Th. Claeys et D. Dejonghe, "Gebruik van *e-mail* en internet op de werkplaats en controle door de werkgever", *J.T.T.*, 2001, p. 121 ; Trib. trav. Hasselt, 21 octobre 2002, *Chron. D.S.*, 2003, p. 197 ; S. van Wassenhove, M. De Leersnyder, G. Chuffart, *Nouvelles Technologies et leur impact sur le droit du travail*, Heule, Bruxelles, 2003, p. 46.

28 J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, p. 47 ; E. Carlier et G. Albert, « L'instauration d'un plan de sécurité dans l'entreprise et le droit au respect de la vie privée », *in Vie privée du travailleur et prérogatives patronales*, *loc. cit.*, p. 2001 ; H. Barth, « Contrôle de l'employeur de l'utilisation privée que font les travailleurs des nouvelles technologies de l'information et de la communication au lieu de travail », *J.T.T.*, 2002, p. 173. En ce sens, voyez également : C. trav. Bruxelles, 3 mai 2006, R.G. nº 45.922, www.cass.be.

29 H. Barth, « Contrôle de l'employeur de l'utilisation privée que font les travailleurs des nouvelles technologies de l'information et de communication au lieu de travail », *J.T.T.*, 2002, p. 173.

Elle pourrait même être requise dans certains cas. On verra qu'en droit belge, certaines ingérences, telle la prise de connaissance de communications électroniques, ne peuvent se faire sans le consentement des personnes concernées[30].

§ 2. Principe de finalité

14. Du libellé de l'alinéa 2 de l'article 8 de la C.E.D.H. se déduit également un *principe de finalité* aux termes duquel l'ingérence doit, en outre, poursuivre un des buts légitimes qui y sont limitativement énoncés. Ainsi, une ingérence peut elle éventuellement être justifiée lorsqu'elle vise à prévenir une infraction pénale (vol, pédophilie, abus de confiance,…), la protection des droits et libertés d'autrui (respect des instructions de l'employeur, protection contre le harcèlement,…) ou encore le respect de la morale (respect des bonnes mœurs,…)[31].

§ 3. Principe de proportionnalité

15. Enfin, l'ingérence doit être une mesure « nécessaire, dans une société démocratique, à la poursuite de ce but ». La Cour européenne des droits de l'homme a précisé à cet égard, dans un arrêt *Olsson c. Suède* que « […] la notion de nécessité implique une ingérence fondée sur un besoin social impérieux et notamment proportionné au but légitime recherché […] »[32]. Il en résulte que non seulement la mesure d'ingérence doit être utile à la réalisation du but poursuivi mais qu'elle doit, de surcroît, être la moins dommageable pour la réalisation de ce but. Ce *principe de proportionnalité* invite donc à vérifier « si un juste équilibre a été ménagé entre ce but et le droit en cause, tenant compte de son importance et de l'intensité de l'atteinte portée »[33].

16. Dans le cadre de ce contrôle de proportionnalité, le droit au respect de la vie privée peut être mis en balance avec d'autres droits fondamentaux, et même, selon J.-Fr. Neven, avec les intérêts économiques de l'employeur[34]. Ainsi, selon cet auteur – qui s'appuie également sur la thèse de F. Hendrickx à cet égard –, les intérêts de l'employeur par rapport à une ingérence déterminée dans la vie privée d'un travailleur peuvent être directement confrontés, « en

---

30 J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, pp. 45-46.

31 *Cf.* H. Barth, « Contrôle de l'employeur de l'utilisation privée que font les travailleurs des nouvelles technologies de l'information et de communication au lieu de travail », *J.T.T.*, 2002, p. 173.

32 Cour eur. D.H., arrêt *Olsson c. Suède*, 24 mars 1988, Série A, n° 130, pp. 31-32, § 67 ; Cour eur. D.H., arrêt *Dudgeon*, 22 octobre 1981, série A, p. 15, § 51.

33 V. Coussirat-Coustere, « Article 8 § 2 », *in La convention européenne des droits de l'homme. Commentaire article par article*, L.-E. Pettiti, E. Decaux et P.-H. Imbert (dir.), Paris, Economica, 1995, p. 338.

34 J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, éd. du Jeune Barreau de Bruxelles, 2005, pp. 30-32.

évitant que le droit au respect de la vie privée ne soit « subordonné » au pouvoir d'autorité du travailleur »[35]. L'ingérence ne pourrait dès lors être discrétionnaire et se fonder uniquement sur l'exercice de l'autorité de l'employeur mais devrait être justifiée au regard des intérêts de l'entreprise.

2. L'article 22 de la Constitution

a. Objet de la protection

17. Aux termes de 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 ». Ce droit protège également la correspondance échangée par courrier électronique[36].

L'article 22, introduit lors d'une modification de la Constitution réalisée en 1994, transpose en droit belge l'article 8 de la C.E.D.H. Il ressort clairement des travaux préparatoires, que le législateur a voulu mettre en concordance l'article 22 avec l'article 8 de la C.E.D.H. de sorte qu'il convient de donner à cette disposition la même portée que l'article 8 de la C.E.D.H., sauf en ce qui concerne l'exigence de légalité puisque, comme nous l'évoquerons, une loi au sens formel du terme est exigée par ledit article 22. Pour déterminer ce qui constitue ou non une ingérence dans la vie privée au sens de l'article 22, on peut donc notamment avoir égard à la jurisprudence relative à l'article 8 de la C.E.D.H.

b. Effets de l'article 22

18. Si à l'instar de l'article 8 de la C.E.D.H. l'article 22 affirme l'existence du droit au respect de la vie privée, on constate une différence de taille entre les deux dispositions. Alors qu'une ingérence dans la vie privée d'autrui peut résulter de toute norme claire et accessible, l'article 22 n'autorise une telle ingérence que *dans les cas et conditions fixés par la loi* au sens formel du terme. L'article 22 vise à déterminer qui est compétent pour édicter des normes générales induisant des ingérences dans la vie privée. Il y répond en indiquant que seul le législateur fédéral, régional ou communautaire est compétent[37].

---

35 *Ibid.*

36 C. trav. Liège, 23 mars 2004, *R.R.D.*, 2004, p. 73. L'article 29 de la Constitution ne lui est en revanche pas applicable (Voy. par exemple en ce sens l'analyse de P. Degouis et S. van Wassenhove, *Nouvelles technologies et impact sur le droit du travail*, Courtrai, UGA, 2010, pp. 26-27.

37 E. Degrave, « L'article 22 de la Constitution et les traitements de données à caractère personnel », *J.T.*, 2009, p. 366. C'est en ce sens que nous estimons que de telles ingérences ne peuvent être créées dans un arrêté royal rendant obligatoire la C.C.T. nº 81 et qui déroge à une loi, en l'occurrence l'article 124 de la loi du 13 juin 2005 (cf. section 5.B.d).

À cet égard, dans un arrêt du 19 juillet 2005, la Cour constitutionnelle (à l'époque, Cour d'arbitrage) a constaté que : « Bien que, en utilisant le terme 'loi', l'article 8.2 de la Convention européenne précitée n'exige pas que l'ingérence qu'il permet soit prévue par une 'loi', au sens formel du terme, le même mot 'loi' utilisé à l'article 22 de la Constitution désigne une disposition législative. Cette exigence constitutionnelle s'impose au législateur belge, en vertu de l'article 53 de la Convention européenne, selon lequel les dispositions de la Convention ne peuvent être interprétées comme limitant ou portant atteinte aux droits de l'homme et aux libertés fondamentales reconnues notamment par le droit interne »[38].

Ainsi, au regard de l'article 22 de la Constitution, et à la différence de l'article 8 de la C.E.D.H., un simple règlement de travail ou contrat de travail ne peut à lui seul permettre une atteinte à la vie privée du travailleur si celle-ci n'est pas prévue dans une loi.

Une disposition prévoyant une ingérence dans la vie privée des citoyens prise dans un arrêté royal pourrait donc également être déclarée inconstitutionnelle[39]. Cette particularité du droit belge donne lieu à une discussion quant à la possibilité de recourir à des C.C.T.[40] pour réglementer des problématiques impliquant le droit au respect de la vie privée des travailleurs[41].

Dans un arrêt du 18 mars 2010, la Cour constitutionnelle a encore rappelé le principe de légalité dans un litige portant sur le traitement de données à caractère personnel en énonçant que : « En réservant au législateur compétent le pouvoir de fixer dans quels cas et à quelles conditions il peut être porté atteinte au droit au respect de la vie privée et familiale, l'article 22 de la Constitution garantit à tout citoyen qu'aucune immixtion dans ce droit ne pourra avoir lieu qu'en vertu de règles adoptées par une assemblée délibérante,

---

38 C.A., 19 juillet 2005, R.G. n° 131/2005, B.5.2).

39 J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles, » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, éd. du Jeune Barreau de Bruxelles, 2005, pp. 35 à 37.

40 On pense aux C.C.T. n^{os} 68 (sur la vidéosurveillance), 81 (sur le contrôle des données de communication électronique en réseau), 89 (sur la fouille) et 100 (sur les contrôles en matière d'utilisation de drogues et d'alcool).

41 P. de Hert, O. de Schutter et B. Smeesters, « Emploi, vie privée et surveillance. À propos de la convention collective du travail no 68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail », *J.T.T.*, 1/2001, pp. 9-10 ; G. Demez, « La preuve en droit du travail : protection de la vie privée et nouvelles technologies. Du contremaître à la surveillance », *in Questions de droit social*, Formation permanente CUP, n° 56, 2002, pp. 320-321 et réf. citées ; O. Moreno et S. van Koekenbeek, « Les mutations de la vie privée au travail », *Orientations*, n° 35, 2005, p. 23 ; J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, éd. du Jeune Barreau de Bruxelles, 2005, pp. 34 et s.

démocratiquement élue. Une délégation à un autre pouvoir n'est pas contraire au principe de légalité, pour autant que l'habilitation soit définie de manière suffisamment précise et porte sur l'exécution de mesures dont les éléments essentiels sont fixés préalablement par le législateur ».[42]

Si une délégation est donc possible, elle devrait être expresse et encadrée par le législateur[43]. On peut douter que du fait que la loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions paritaires réponde à ce degré de précision[44].

Ceci étant, on notera qu'à notre connaissance les juridictions de fond ont appliqué ces C.C.T. sans remettre en cause leur conformité à la Constitution, comme elles seraient pourtant habilitées à le faire en application de l'article 159 de la Constitution[45].

3. Conséquence de l'application cumulative des articles 8 de la C.E.D.H. et de l'article 22 de la Constitution

19. Lorsqu'il s'agit de déterminer dans quelle mesure une ingérence dans la vie privée d'un citoyen dans celle d'un autre peut intervenir, il y aura lieu de se référer à la législation belge réglementant spécifiquement ces ingérences. En application de l'article 22, le législateur peut prévoir certaines ingérences et ce sont ces dispositions dont pourront se prévaloir les justiciables. Ces dispositions doivent elles-mêmes toujours être conformes à l'article 8 C.E.D.H. et respecter les exigences de précision, d'accessibilité de prévisibilité du dit article 8 de la C.E.D.H.[46].

Si des ingérences doivent être prévues dans une loi au sens de l'article 22 de la Constitution, elles doivent également être prévues de manière assez précise pour ne pas déjouer ses attentes légitimes des personnes concernées par

---

42 C.C., 18 mars 2010, R.G. nº 29/2010, B.16.1.

43 O. Moreno et S. Van Koekenbeek estiment toutefois qu'une habilitation légale ne serait pas nécessaire lorsque les limitations au droit à la vie privée proviennent d'une directive européenne dont les règles sont appliquées dans une C.C.T. (O. Moreno et S. van Koekenbeek., « Les mutations de la vie privée au travail », *Orientations*, nº 35, 2005, p. 17).

44 *Ibidem*.

45 Voy. sur la question du contrôle de légalité des C.C.T., J.-Fr. Neven et P. Joassart, « Légalité des conventions collectives de travail », *in Les 40 ans de la loi du 5 décembre 1968 sur les conventions collectives de travail*, Bruxelles, Bruylant, 2008, voy. spéc. p. 94 sur l'exigence de conformité avec les dispositions de impératives l'ordre étatique.

46 Voy. Projet de loi relatif 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.*, Sénat, session 1993-94, 16 décembre 1993, nº 100/4-5°, p. 4, où il est fait remarqué que l'on « accepte en pratique que les employeurs portent atteinte au principe de la vie privée des travailleurs (contrôle médical, fouilles, contrôle de l'emploi du téléphone, caméras.).

celles-ci[47], d'où la question par exemple du caractère suffisamment précis et prévisible de la loi du 3 juillet 1978 évoquée ci-avant.

Par ailleurs, pour déterminer dans quelle mesure un employeur peut poser des actes impliquant une ingérence dans la vie privée de travailleurs, l'article 8 de la C.E.D.H. peut en fournir les balises. J.-Fr. Neven explique à cet égard que « L'obligation faite aux états parties à la Convention d'adopter les mesures destinées à prévenir les violations des droits fondamentaux inclut donc les rapports entre particuliers et s'impose au législateur mais aussi aux tribunaux à qui il incombe, en cas d'encadrement normatif insuffisant, de sanctionner les comportements contraires aux droits garantis par la C.E.D.H., en s'appuyant si nécessaire exclusivement sur cette dernière[48] ». Il appartient alors au Juge de sanctionner le non respect de cette disposition en constatant, le cas échéant, la nullité d'un acte juridique ou l'existence d'un fait générateur de responsabilité[49]. Les juridictions du travail font d'ailleurs généralement mention de cette disposition lorsqu'elles examinent la violation ou non de la vie privée du travailleur[50].

Section 3
La protection des communications électroniques

A. Notions

20. Avec la convergence des technologies, il est aujourd'hui fait référence à l'usage du téléphone (mobile ou fixe), de l'e-mail et de l'internet ainsi que de la communication par SMS ou même le repérage par satellite (par exemple, par le biais d'un GPS) sous le vocable de « communications électroniques ». Ce terme désigne toute transmission de *tous types de signaux (voix, images, etc.) autres que ceux de la radiodiffusion ou de la télévision*, indépendamment du médium utilisé et comprenant l'acheminement « par câble, par voie hertzienne, par moyen optique ou par d'autres moyens électromagnétiques, comprenant les réseaux satellitaires, les réseaux terrestres fixes (avec communication de circuits ou de

---

47 J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Ed. Jeune Barreau de Bruxelles, pp. 45-47.

48 *Ibid.*, p. 38.

49 *Ibid.*, p. 39.

50 Voyez par exemple : Trib. trav. Hasselt, 21 octobre 2002, R.G. n° 2020348, www.cass.be ; C. trav. Anvers, 1er octobre 2003, R.G. n° 2020381, www.cass.be ; C. trav. Bruxelles (3e ch.), 10 février 2004, R.G. n° 44002, www.cass.be ; Trib. trav. Bruxelles, 14 décembre 2004, *Computerrecht*, 2005, p. 313 ; C. trav. Anvers, 15 décembre 2004, R.G. n° 2004-0295, www.cass.be.

paquets, y compris l'internet) et mobiles, les systèmes utilisant le réseau électrique, pour autant qu'ils servent à la transmission de signaux, les réseaux utilisés pour la radiodiffusion sonore et télévisuelle et les réseaux câbles de télévision » [51].

Il en résulte que, lorsque l'on fait référence au secret des communications électroniques, les dispositions évoquées valent tout autant pour les communications téléphoniques ou par fax, que pour la connexion à une page internet, ou pour la correspondance par e-mail, ou la consultation de SMS [52].

21. On remarque que certains textes légaux visent le contenu des communications électroniques alors que d'autres visent les données de communication de la communication elle-même. Ainsi, la C.C.T. nº 81 dispose-t-elle dans son préambule que « seules les données de communication électroniques pourront être individualisées. Leur contenu ne pourra l'être sauf aux parties et certainement au travailleur à donner son accord conformément au prescrit des lois du 21 mars 1991 et 8 décembre 1992 précitées ». La notion de « contenu des communications électroniques » est également utilisée par les articles 314*bis* et 259*bis* du Code pénal (voir point B,1 de la présente section). Notons que l'article 124 de la loi du 13 juin 2005 (voir point B.2 de la présente section) utilise quant à lui le concept de « prise de connaissance de l'existence d'une communication électronique », lequel ne se recoupe pas facilement avec ceux de « contenu » et « de données de communication électroniques ».

Les textes précités concernent tous la prise de connaissance de communications électroniques mais nous verrons que la prise de connaissance du contenu d'une communication ne se fait pas nécessairement aux mêmes conditions que celle des données de communication.

---

51 Directive 2002/21/CE, art. 1 (a) ; voy. également la définition de la notion de service de communication électronique à l'article 2, 5° de la loi du 13 juin 2005 relative aux communications électroniques.

52 J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, p. 84. Le terme « communications électroniques » utilisé dans la loi du 13 juin 2005 remplace l'ancienne appellation de « télécommunications » de la loi du 21 mars 1991 (« loi *Belgacom* »). Voy. le commentaire de l'Observatoire des droits de l'internet sur le secret des communications et la protection de la vie privée, http://www.internet-observatory.be/internet_observatory/pdf/legislation/cmt/law_be_1991-03-21_cmt_fr.pdf : « Le terme "télécommunications" doit et doit également être interprété d'une façon large, et est défini dans l'article 68, 4° de la loi Belgacom comme toute "transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radioélectricité, signalisation optique ou un autre système électromagnétique". Ceci ne couvre donc pas seulement la téléphonie et la télégraphie, mais aussi les formes de communication un peu plus modernes, comme le courriel, le web, le chat, le *home shopping*, le *télébanking*, les logiciels *peer-to-peer*… ».

22. Bien qu'il n'y ait pas de définition légale du concept de « données de communication électroniques », il semble bien que ce terme vise les données relatives aux communications électroniques qui permettent l'acheminement d'une communication électronique transitant par réseau telles l'adresse e-mail de l'expéditeur et du destinataire, l'heure de l'envoi et de la réception, les données de routage, la taille du message, la présence de pièces jointes, etc.[53]. Ainsi, le corps du message ou le contenu de la page web relèvent du contenu de la communication tandis que l'adresse ou le numéro de téléphone des expéditeurs ou destinataires d'un message tout comme l'adresse de la page web peuvent être considérés comme des données de communication.

On peut cependant critiquer cette distinction pour au moins deux raisons. D'une part, l'absence de définition légale de ces deux termes peut en rendre les contours flous et difficiles à cerner. Ainsi, on peut se demander si l'objet d'un e-mail doit être considéré comme le contenu de cet e-mail ou comme une information relative à l'e-mail lui-même, dès lors que l'objet n'est précisément pas dans le corps du texte. De la même manière, si la taille d'un e-mail ne peut être considérée comme appartenant au contenu d'une communication électronique, il ne nous paraît pas si évident de ranger la taille d'un message électronique dans la catégorie des données de communication, sauf à considérer que tombe dans cette catégorie toute information qui ne relève pas de son contenu.

D'autre part, la distinction peut paraître artificielle, dès lors que connaître l'adresse IP d'un site internet auquel un travailleur se serait connecté revient forcément à pouvoir en consulter le contenu facilement alors que, strictement parlant, une adresse IP est une donnée de communication puisqu'elle identifie la localisation d'un ordinateur distant sur internet et permet l'acheminement de l'information.

Signalons encore que, parmi les données de communication, le législateur a identifié deux types particuliers de données de communication électroniques qui entrent en ligne de compte dans le contexte de la fourniture des services de communications électroniques. Il s'agit des données de trafic et des données de localisation qui seront évoquées dans le cadre de services de localisation du travailleur par satellite[54].

---

53 O. Rijckaert, « Le contrat de travail face aux nouvelles technologies », *Orientations*, 2000, p. 210. Pour un cas d'application voyez : C. trav. Bruxelles, 10 février 2004, R.G. nº 44.002, www.cass.be.

54 Art. 2, 6° et 7° de la loi du 13 juin 2005 relative aux communications électroniques.

B. Le secret des communications électroniques

23. Aux dispositions qui consacrent le droit au respect de la vie privée, il convient d'ajouter celles dédiées spécifiquement aux communications électroniques[55].

La réglementation belge relative aux communications électroniques est issue du droit européen. La directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (la « directive 2002/58/EC » ou la « directive »)[56] a, en effet, été adoptée en vue protéger le droit au respect de la vie privée et d'assurer la libre circulation des données dans le secteur particulier des communications électroniques[57]. Elle fait partie d'un paquet de cinq directives destiné à reformer le cadre réglementaire régissant les services et réseaux de communications électroniques dans la Communauté.

Cette directive a été transposée en droit belge dans la loi du 13 juin 2005 sur les communications électroniques. Le principe du secret des communications y est défini à l'article 124 et les exceptions aux articles 125 et 128 de la loi. Les articles 124 et 125 remplacent les articles 109*ter* D et 109*ter* E de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (loi dite *Télécom* ou encore *Belgacom*) qui ont été abrogées par la loi du 13 juin 2005 relative aux communications électroniques[58]. Nous ne traiterons pas du prescrit de ces dispositions anciennes si ce n'est dans ce qu'elles peuvent nous renseigner sur la portée des dispositions actuellement en vigueur.

24. En sus de cette loi, subsistent les articles 314*bis* et 259*bis* du Code pénal qui prohibent également certains actes de prise de connaissance des communications électroniques.

---

55 Si l'on a fait souvent référence à l'article 29 de la Constitution comme obstacle à la prise de connaissance de communications électroniques (principalement les e-mails), il nous semble qu'au contraire cette disposition ne trouve pas à s'appliquer dans ce contexte dès lors qu'elle vise les lettres confiées à un organisme postal (*cf.* en ce sens : Th. Claeys et D. Dejonghe, « Gebruik van e-mail en internet op de werkplaats en controle door de werkgever », *J.T.T.*, 2001, p. 129).

56 Ou « Directive vie privée et communications », *J.O.C.E.*, nº L 20, 31 juillet 2002, pp. 0037-0047.

57 La directive 2002/58/CE remplace la 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, *J.O.C.E.*, nº L 024, 30 janvier 1998, pp. 0001-0008. Elle a elle-même été amendée par la directive 2009/136/CE du 25 novembre 2009 (*J.O.C.E.*, nº L337, 18 décembre 2009, pp. 11-36).

58 La loi du 13 juin 2005 transpose en droit belge les directives du paquet de cinq directives destiné à reformer le cadre réglementaire régissant les services et réseaux de communications électroniques dans la Communauté dont la directive 2002/58/CE Vie privée et communications électroniques.

À ce propos, il est opportun de souligner que la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées[59] avait modifié la portée des dispositions contenues dans la loi du 21 mars 1991 pour qu'elles ne portent plus sur le contenu des communications mais sur les données de communication. À partir de 1994, on a donc vu s'affirmer en doctrine et en jurisprudence, une distinction entre la réglementation de la protection du contenu des communications, d'une part, et celle des données de communication, d'autre part. Le contenu était protégé par les articles 314*bis* et 259*bis* du Code pénal tandis que les données de communication l'étaient par la loi du 21 mars 1991[60].

Nous verrons que le libellé ambigu de l'article 124 de la loi du 30 juin 2005 met à mal cette distinction et que l'on peut se demander si, à présent, le contenu des communications n'est pas régi à la fois par les dispositions précitées du Code pénal et par l'article 124.

1. Les articles 314*bis* et 259*bis* du Code pénal

25. L'article 314*bis* est ainsi libellé :

> « § 1. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents francs à dix mille francs ou d'une de ces peines seulement, quiconque :
>
> 1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications ;
>
> 2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.
>
> § 2. Sera puni d'un emprisonnement de six mois à deux ans et d'une amende de cinq cents francs à vingt mille francs ou d'une de ces peines seulement, quiconque détient, révèle ou divulgue sciemment à une autre personne le contenu de communications ou de télécommunications privées, illégalement écoutées ou enregistrées, ou dont il a pris connaissance illégalement, ou utilise sciemment d'une manière quelconque une information obtenue de cette façon.
>
> Sera puni des mêmes peines quiconque, avec une intention frauduleuse ou à dessein de nuire, utilise un enregistrement, légalement effectué, de communications ou de télécommunications privées.

---

59 *M.B.*, 25 janvier 1995, p. 01542.

60 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 188.

> § 2*bis*. Sera puni d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, celui qui, indûment, possède, produit, vend obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1er.
>
> § 3. La tentative de commettre une des infractions visées aux §§ 1er, 2 ou 2*bis* est punie comme l'infraction elle-même.
>
> § 4. Les peines prévues aux §§ 1er à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passés en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 259*bis*, §§ 1er à 3.»

L'article 259*bis* a un objet similaire si ce n'est que l'interdiction s'adresse aux officiers, fonctionnaires publics, dépositaires ou agents de la force publique qui poseraient de tels actes à l'occasion de l'exercice de leurs fonctions.

a. Actes prohibés

26. Le simple fait de faire écouter, de faire enregistrer ou de faire prendre connaissance d'une communication, qu'il s'agisse d'un fax ou d'un e-mail, est donc interdit sans qu'il ne soit pas nécessaire qu'on ait pris connaissance de ce qui fut intercepté.

Les articles 314*bis* et 259*bis* du Code pénal impliquent toutefois l'intervention d'un dispositif installé pour écouter une conversation. Le fait d'entendre tout ou partie d'une conversation téléphonique parce qu'il se trouve à portée de voix ou lorsque le haut parleur d'un des interlocuteurs est mis, fût-ce sans que les parties à la conversation ne s'en aperçoivent, n'est donc pas visé dans cette disposition[61].

27. Notons encore que ces dispositions exigent dans certains cas de figure un élément intentionnel lors de la commission de l'infraction. Sans évoquer ce qu'implique cet élément intentionnel, la Cour du travail d'Anvers analyse si oui ou non on peut considérer que l'élément moral de l'infraction était présent dans le chef du responsable IT qui avait effectué un contrôle sur les communications du travailleur[62]. La cour estime que le travailleur ayant signé un document par lequel il marquait son accord avec les dispositions du règlement IT de l'entreprise prévoyant des contrôles, il en avait accepté l'éventualité. Elle

---

61 Voy. à cet égard : F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 190.

62 C. trav. Anvers (sect. Hasselt), 2 septembre 2008, *DAOR*, 2010, p. 336, note A. Van Bever ; *Orientations*, 2008 (reflet I. Plets), liv. 9, p. 261. Pour un commentaire de cette décision, voyez également : K. Rosier, « Le cybercontôle des travailleurs contrôlé par le Juge », *Orientations*, 2009, pp. 22 et s.

considère que dans ces conditions, on ne peut soutenir que l'élément moral de l'infraction est présent.

b. Informations protégées

28. Par ailleurs, les termes « communications » ou « télécommunications » reçoivent une acception très large et comprennent les communications écrites ou orales que ce soit par le biais du téléphone, de talkie-walkie, de communications électroniques par internet, par SMS, le contenu des pages consultées ou d'autres formes de téléphonie par internet[63].

Ces dispositions visent la communication ou la télécommunication : quelle portée donner concrètement à ces termes ?

Selon F. Hendrickx, l'existence de la communication est nécessairement visée[64]. En revanche, on peut se demander si les données de communication sont également concernées. La dichotomie voulue entre contenu et donnée de communication nous incite à répondre par la négative, sauf à considérer que certaines données relatives à la communication (comme par exemple l'adresse du destinataire ou de l'expéditeur d'un courrier électronique ou la date et l'heure de la communication) qui apparaissent dans le message font également partie du contenu. Dès lors, le simple enregistrement des adresses des correspondants ou de l'adresse des sites internet visités ne tombe pas dans le champ d'application de cette disposition[65].

29. La protection ne vise que les communications privées. Par « communications privées », on vise les communications qui ne sont pas destinées à être « entendues » – ou plutôt dans le contexte des communications électroniques « lues » – par tout un chacun[66].

Ceci implique que le fait qu'une communication intervienne dans un contexte professionnel ne fait pas obstacle à ce qu'elle puisse être qualifiée de « privée »[67].

c. Période de la protection limitée à la transmission

30. Par ailleurs, la protection relative au contenu des communications électroniques n'intervient que *pendant la transmission*. Dès lors que la transmission

---

63 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 189.

64 *Ibidem*, p. 194.

65 Th. Claeys et D. Dejonghe, « Gebruik van *e-mail* en internet op de werkplaats en controle door de werkgever », *J.T.T.*, 2001, pp. 126-127.

66 Th. Verbiest et É. Wery, *Le droit de la société de l'information. Droits européen, belge et français*, Bruxelles, Larcier, 2001, p. 188.

67 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 190 ; C. trav. Anvers, 15 décembre 2004, R.G. n^{os} 2004-0295, www.cass.be.

du courrier électronique est achevée, la protection du contenu n'existe plus. Cela ne veut pas dire pour autant que l'on pourrait prendre connaissance ou faire un usage d'informations glanées grâce à une interception prohibée des communications pendant la transmission. En leur deuxième paragraphe, les articles 314*bis*/259*bis* érigent également en infraction un tel usage. Ceci dit, cette limitation a eu pour conséquence que l'enregistrement ou la prise de connaissance du contenu d'une communication intervenant après la fin de la transmission n'est pas visée par ces dispositions. Il est donc primordial de pouvoir déterminer à quel moment cette transmission prend fin.

Certains auteurs considèrent implicitement que l'enregistrement automatique d'une copie du courrier électronique sur le serveur e-mail d'une entreprise avant sa « distribution » à son destinataire final intervient pendant la transmission[68]. D'autres sont, par contre, d'avis que la transmission se termine précisément dès le moment où l'e-mail est copié, soit sur le serveur de l'employeur, soit sur le disque dur de l'employé[69].

31. En toute hypothèse, il nous faut constater que, dans la plupart des cas, la prise de connaissance d'un courrier électronique interviendra alors que le courrier est parvenu à son destinataire, que celui-ci ait ou non ouvert ledit courrier. Les interdictions des dispositions en question ne seront dès lors pas applicables[70].

Cette disposition ne fait donc pas obstacle à un contrôle du contenu des e-mails qui peuplent la boîte e-mail d'un travailleur, pas plus que la consultation des SMS stockés dans la mémoire d'un GSM à usage professionnel.

Les articles 314*bis* et 259*bis* ont été manifestement pensés par rapport au cas des communications téléphoniques. Leur application stricte aux communications électroniques exclut la protection contre une prise de connaissance du contenu aux communications électroniques parvenues à leur destinataire, ce qui ne satisfait pas tous les auteurs[71].

---

68 P. De Hert, « C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en *e-mail* », *R.W.*, 2002-2003, nº 33, p. 1285 et O. Rijckaert, « Le contrat de travail face aux nouvelles technologies », *Orientations*, 2000, p. 208.

69 M. Lauvaux, V. Simon et D. Stas de Richelle, *Criminalité au travail*, Bruxelles, Kluwer, 2007, p. 99.

70 Pour une application voyez : C. trav. Anvers, 8 janvier 2003, R.G. nº 2020255, www.cass.be.

71 Voyez à cet égard P. De Hert qui en appelle à une interprétation évolutive de cette disposition. (P. De Hert, « C.A.O. nr. 81 en advies nr. 10/2000 over controle van internet en *e-mail* », *R.W.*, 2002-2003, pp. 1284 et 1285.

2. Les articles 124 et 125 de loi du 13 juin 2005 sur les communications électroniques

L'article 124 de la loi du 13 juin 2005 relative aux communications électroniques (et qui remplace l'article 109*ter* D de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (loi *Télécom*)) prévoit que :

> « S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut :
> 1° prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement ;
> 2° identifier intentionnellement les personnes concernées par la transmission de l'information et son contenu ;
> 3° sans préjudice de l'application des articles 122 et 123 prendre connaissance intentionnellement de données en matière de communications électroniques et relatives à une autre personne ;
> 4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non ».

a. Quelles sont les communications visées ?

La protection s'appuie sur le concept de tiers à la communication, qui n'a pas la qualité de destinataire de la communication. Il est alors fait une distinction entre communication publique et communication privée pour cerner le champ d'application de la protection. La communication publique est celle destinée à tous tandis que la communication privée n'est destinée qu'à un certain nombre de personnes[72].

Ainsi, tous les e-mails ou SMS échangés dans un contexte de travail revêtiront un caractère privé[73] et les personnes non destinataires des communications sont visés par l'interdiction de poser les actes prohibés par l'article 124.

Certaines décisions de jurisprudence[74], lorsqu'elles indiquent que l'employeur ne peut consulter des e-mails reçus ou envoyés par le travailleur, se plaisent à souligner que la protection ne vaut que lorsque celle-ci revêt un

---

72 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés multiples contraintes », *Orientations*, 2005, n° 35, p. 44.

73 J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, p. 84.

74 Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. n° 360.454, www.cass.be ; C. trav. Liège, 20 mars 2006, *R.R.D.*, 2006, pp. 89-101, note K. Rosier et S. Gilson ; Trib. trav. Malines, 22 octobre 2002, *Chron. D.S.*, 2003, pp. 201-203.

caractère privé. Elles peuvent, ce faisant, laisser entendre qu'une telle ingérence aurait par contre été admissible si les e-mails avaient été de nature strictement professionnelle[75].

C'est ainsi que, dans un jugement du 19 mars 2008, le Tribunal du travail de Liège indique que «le caractère mixte d'un échange de correspondance lui enlève son caractère professionnel, de sorte que les principes constitutionnels du secret des lettres et du respect de la vie privée doivent s'appliquer dans toute leur rigueur»[76].

32. Cependant, ceci ne nous paraît pas exact dès lors que la loi n'opère nullement une telle distinction. Nous verrons toutefois que la C.C.T. nº 81 contient une affirmation dans le préambule aux termes de laquelle «lorsque l'objet et le contenu des données de communication électroniques en réseau ont un caractère professionnel non contesté par le travailleur, l'employeur pourra les consulter sans autre procédure» et l'article 11, al. 3 la reproduit au sein de la Convention. Dans un arrêt du 15 décembre 2004[77], la Cour du travail d'Anvers constate que cette distinction est contraire à l'article 8 de la C.E.D.H. ainsi qu'aux articles 314*bis* du Code pénal et à l'article 109*ter* D de la loi du 21 mars 1991 et à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

b. Quels sont les données protégées ?

§ 1er. L'identité des personnes concernées

33. L'article 124, en son deuxième alinéa vise expressément l'identité des personnes concernées tant par la transmission que par son contenu. Il en résulte qu'est interdite la consultation des données relatives à l'identité de l'expéditeur et du ou des destinataires des messages. La référence au contenu implique, si l'on veut donner une portée utile à cette précision, que les personnes qui sont concernées par le contenu (par exemple, citées dans le courrier électronique) seraient elles aussi visées.

§ 2. Les données de communication électroniques

34. Le troisième alinéa a trait, quant à lui, aux données de communication électroniques, en ce incluses les données de trafic et les données de localisation définies aux articles 122 et 123 de la loi du 13 juin 2005.

---

75 Voyez en ce sens, F. Lagasse, «La vie privée et le droit du travail», *Chron. D.S.*, 1997, p. 424.; C. trav. Bruxelles (4e ch.), 3 mai 2006, R.G. nº 45.922, www.cass.be.

76 Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. nº 360.454, www.cass.be.

77 C. trav. Anvers, 15 décembre 2004, R.G. nº 2004-0295, www.cass.be.

Comme indiqué ci-avant, par « données de communication électroniques », on entend les données relatives aux communications électroniques qui transitent par réseau telles l'adresse e-mail de l'expéditeur et du destinataire, l'heure de l'envoi et de la réception, les données de routage, la taille du message, la présence de pièces jointes, etc.[78].

Le constat opéré à l'époque où l'article 109*ter* D de la loi *Télécom* était encore en vigueur et au terme duquel l'interdiction de la prise de connaissance des données de communication constituait un obstacle majeur à la prise de connaissance du contenu reste donc d'application.

En effet, la prise de connaissance du contenu d'une communication entraînera souvent la prise de connaissance des données de communication (adresse électronique de l'expéditeur et du destinataire, date et heure de la communication,…) si bien que l'interdiction - non limitée à la durée de la transmission - de la prise de connaissance des données de communication constituera alors un obstacle à la prise de connaissance du contenu de la communication même après la transmission.

§ 3. L'information transmise ou la transmission de l'information ?

35. L'article 124, 1° de la loi du 13 juin 2005 vise la prise de connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique.

C. de Terwangne, J. Herveg et J.-M. Van Gyseghem relèvent, à propos de ce premier aliéna que « Il semble, de prime abord, ne viser que les données liées au transport des communications et non le contenu de celles-ci »[79]. L'interprétation de l'alinéa premier de l'article 124 précité nous paraît effectivement des plus malaisées. Il est étonnant que le libellé vise « la prise de connaissance de l'existence d'une information » et non de l'information elle-même, ce qui aurait permis d'en déduire que le contenu de la disposition était assurément visé. Les travaux préparatoires n'apportent aucune précision à cet égard.

Pourtant, l'enregistrement de ces données nous semble se confondre avec les actes visés au troisième alinéa de l'article 124 (données de communication électroniques). On peut dès lors se demander quelle est l'utilité d'une telle

---

78 O. Rijckaert, « Le contrat de travail face aux nouvelles technologies », *Orientations*, 2000, p. 210 ; Pour une application voy. : C. trav. Bruxelles, 10 février 2004, R.G. n° 44002, www.cass.be. À propos des articles qui ont précédés l'article 124 (à savoir l'article 111, 3° devenu l'article 109*ter* D, 3° de la loi du 21 mars 1991), F. Hendrickx estimait toutefois que la protection ne concernait pas en tant que telle toutes les données qui sont généralement connues, comme le nom, l'adresse, etc. de l'utilisateur (F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 188).

79 C. de Terwangne, J. Herveg et J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication*, Bruxelles, Kluwer, 2005, p. 46.

disposition si ce n'est de viser plutôt que le transport, la communication elle-même, en ce compris son contenu.

À notre connaissance, la question n'a pas été abordée en tant que telle par la jurisprudence qui semble considérer pour acquis que l'article 124 fait obstacle à la prise de connaissance du contenu des communications sans s'étendre sur le sujet.

36. Constatons tout d'abord que, à propos de l'ancien article 109*ter* D, 1°, la doctrine considérait que cet alinéa visait l'enregistrement de l'existence de messages de télécommunications en ce compris, par exemple, l'enregistrement de la durée de la conversation téléphonique ou des appels entrants et sortants[80]. De fait, le simple enregistrement de ces données pouvait être d'ailleurs un moyen de contrôler l'utilisation qui est faite par des employés de l'internet ou des e-mails, en notant le nombre d'e-mails envoyés, mais également les sites visités, etc.[81].

37. Inclure dans le champ d'application de l'article 124 le contenu de celle-ci conduirait à étendre la portée de cette disposition par rapport à l'ancien article 109*ter* D dans la mesure où il était classiquement admis que cette disposition visait la protection des données de communication alors que les articles 314*bis* et 259*bis* du Code pénal concernaient le contenu des communications[82].

Compte tenu du champ limité de ces dispositions qui ne prévoyaient une protection que durant la durée de la transmission, la protection du contenu de la communication au-delà de la fin de celle-ci induit assurément une extension

---

80 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 193 ; H. Barth, « Contrôle de l'employeur de l'utilisation privée que font les travailleurs des nouvelles technologies de l'information et de la communication au lieu de travail », *J.T.T.*, 2002, p. 171.

81 La Cour de cassation a, dans un arrêt du 2 mai 1990, considéré que le respect du droit à la vie privée, qui est prévu à l'article 8 de la C.E.D.H., s'oppose à ce que l'on puisse enregistrer aussi bien l'heure que la durée des communications téléphoniques, ainsi que les numéros appelés (Cass., 2 mai 1990, *J.T.*, 1990, p. 469).

82 Ceci ressort du reste des travaux préparatoires de la loi du 30 juin 1994 qui indiquent que les termes « du contenu » ont été expressément supprimés de la disposition (voy. Projet de loi relatif 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., session 1992-93, n° 841/1, p. 31) ; *cf.* article 13, § 2, 1° de la loi du 30 juin 1994. La loi du 21 mars 1991 n'avait en effet trait qu'aux télécommunications tandis que les articles 259*bis* et 314*bis* du Code pénal concernaient, à la fois, les communications ordinaires et les télécommunications ; il y avait donc des possibilités de chevauchements. Pour éviter ces chevauchements, l'ancien article 111, 1° devenu l'article 109*ter* D, 1° de la loi du 21 mars 1991 a été modifié afin qu'il ne soit plus applicable à la prise de connaissance du contenu des télécommunications (F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 188).

notable de la protection du contenu en tant que tel[83]. En effet, la protection créée par l'article 124 précité perdure après que la transmission soit achevée[84]. Les travaux préparatoires de la loi du 13 juin 2005 relative aux communications électroniques précisent d'ailleurs que, dans le cas d'un e-mail, la transmission prend fin dès que le destinataire récupère le message auprès de son fournisseur de service[85].

La portée de l'article 124, 1° reste donc sujette à discussion et les considérations suivantes sont utiles pour alimenter le débat.

i. En faveur de l'inclusion des données de communication dans le champ de la protection de l'article 124…

38. En faveur d'une interprétation incluant le contenu de la communication dans l'assiette de la protection, il convient de pointer tout d'abord, la référence indirecte au contenu de la communication dans les alinéas 1 et 4 de l'article 124 qui inclut l'information (et donc le contenu de la communication) véhiculée par la communication électronique dans le champ de la protection[86].

39. Ensuite, relevons que l'article 124 de la loi du 13 juin 2005 est inséré au sein d'une section intitulée « Secret des communications, traitement des données et protection de la vie privée ». Au regard des termes utilisés, on peut y voir la volonté du législateur d'instituer un secret protégeant les communications électroniques. Or, ce terme assez large vise assurément la communication dans son ensemble et donc également le contenu. Dès lors que l'article 124 est la seule disposition de la section visant à assurer le secret des communications, son interprétation peut être utilement guidée par le titre évocateur d'une protection de toute la communication, visant tant les données de transmission que le contenu de la communication.

40. Par ailleurs, cette intention supposée du législateur est aussi inscrite dans l'exposé des motifs très laconique de la loi qui se borne à commenter l'article 124 dans les termes suivants : « cet article protège le caractère confidentiel des informations transmises via un réseau de communications électroniques ».

---

83 Comme nous le signalions ci-avant, la protection plus forte des données de communications constituait néanmoins un obstacle à l'accès au contenu de la communication.

84 Trib. trav. Bruxelles, 22 juin 2000, *Computerrecht*, 2001/6, p. 311 ; Trib. trav. Hasselt, 21 octobre 2002, R.G. n° 2020348, www.cass.be ; Trib. trav. Bruxelles, 2 octobre 2004, R.G. n° 44002, www.cass.be ; C. trav. Bruxelles, 3 mai 2006, R.G. n° 45922, www.cass.be.

85 Projet de loi relatif aux communications électroniques, *Doc. parl.*, Ch. repr., sess., 2004-2005, n° 1425/001, p. 73.

86 Voyez en ce sens, C. de Terwangne, J. Herveg et J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication*, Bruxelles, Kluwer, 2005, p. 50.

Là encore, l'usage du terme « informations » plaide pour une interprétation large du premier aliéna de l'article 124.

41. Enfin, si l'on a égard à la directive 2002/58/CE que la loi du 13 juin 2005 relative aux communications électroniques est censée transposer[87], on note que l'article 5, § 1er de la directive lu à la lumière du considérant 21 de la directive est limpide :

> « Les États membres garantissent, par la législation nationale, la confidentialité des communications effectuées au moyen d'un réseau public de communications et de services de communications électroniques accessibles au public, ainsi que la confidentialité des données relatives au trafic y afférentes. En particulier, ils interdisent à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés sauf lorsque cette personne y est légalement autorisée, conformément à l'article 15, paragraphe 1 ».

Le considérant 21 précise quant à lui que :

> « Il convient de prendre des mesures pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen de réseaux publics de communications et de services de communications électroniques accessibles au public, *y compris de leur contenu*[88] et de toute donnée afférente à ces communications. La législation nationale de certains États membres interdit uniquement l'accès non autorisé intentionnel aux communications ».

ii. En faveur de l'exclusion du contenu communication dans le champ de la protection de l'article 124…

42. En faveur d'une limitation du champ d'application de l'article 124, on relèvera qu'il est étonnant que les articles 314*bis* et 259*bis* du Code pénal qui régissent spécifiquement la prise de connaissance du contenu des communications n'aient pas été abrogés lors de l'adoption de la loi du 13 juin 2005. Est-ce un oubli ou un acte délibéré du législateur ? Nous n'avons pas les clés pour y répondre. Toujours est-il que cette subsistance fait dire à certains auteurs que « L'article 124 interdit dès lors à tout employeur de prendre connaissance de toutes données transmises par voie de télécommunications. Le contenu des

---

87 L'article 1 de la loi du 13 juin 2005 spécifie clairement qu'elle transpose, entre autres directives européennes, la directive 2002/58 du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications.

88 Souligné par les auteurs.

télécommunications n'est pas visé, il est protégé par d'autres dispositions (art. 314*bis* du Code pénal), il ne s'agit que des données relatives aux télécommunications : identité de l'expéditeur, adresse du site visité, la durée de la communication, etc.»[89].

Cette interprétation peut également être confortée par le fait que le premier alinéa de l'article 109*ter* D n'était pas très éloigné de l'article 124 puisqu'il interdisait « 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 » tandis que le quatrième alinéa interdisait de « révéler ou de faire un 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 ». Or certains auteurs ont donné à l'article 109*ter* D, 1° une portée plus retreinte en considérant que la prise de connaissance du contenu d'une communication électronique impliquait la prise de connaissance de l'existence de celle-ci et ont, partant, interprété cette disposition comme ne visant pas spécifiquement le contenu de la communication[90].

43. Peut-on prêter des intentions différentes au législateur qui parlait hier de « l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature » dans l'article 109*ter* D et aujourd'hui de « l'existence d'informations » dans l'article 124 en admettant que l'article 109*ter* D ne visait pas le contenu alors que l'article 124 l'inclurait désormais dans le champ de la protection ? Comment expliquer cette apparente contradiction ?

On peut donc se demander comment concilier ce constat de similarité entre l'article 109*ter* D et l'article 124 précités avec une volonté supposée du législateur d'étendre le champ de la protection accordée via l'article 124 aux contenus des communications.

44. Une distinction notable entre les deux dispositions peut partiellement offrir une réponse. Il n'est plus requis, dans le processus d'obtention de l'information, d'intention frauduleuse dans le chef de l'auteur de l'acte : il suffit désormais que celui-ci agisse « intentionnellement ». Autrement dit, sous l'empire de l'article 109*ter* D, la doctrine et la jurisprudence confrontés à des hypothèses de prises de connaissance non frauduleuses ne faisaient pas application de ce premier aliéna au libellé obscur. Il était généralement référé à l'article 109*ter* D,

---

89 M. Lauvaux, V. Simon et D. Stas de Richelle, *Criminalité au travail*, Bruxelles, Kluwer, 2007, p. 101 ; voy. dans le même sens : J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, p. 85.

90 J. Dumortier, « Internet op het werk, controlerechten van de werkgever », *Or.*, 2000 p. 37 ; F. Hendrickx, *Electronisch toezicht op het werk, internet en camera's*, Ced. Samson, 2001, pp. 90-91.

alinéa 3 relatif aux données de communication qui ne requérait qu'un élément intentionnel et non une intention frauduleuse[91].

iii. Conclusions

45. Il n'est pas exclu, nous semble-t-il, que le problème de deux champs d'application distincts de l'article 314*bis* et de l'ancien article 109*ter* D soit tout simplement resté hors des préoccupations du législateur. Le législateur se serait tout simplement contenté de transposer l'article 5, § 1er de la Directive 2002/58/CE sans avoir égard aux enjeux doctrinaux et jurisprudentiels qui précédaient cette transposition.

Ceci étant, il reste que la coexistence des articles 314*bis* et 259*bis* du Code pénal, d'une part, et l'article 124, d'autre part, ne paraît plus justifiée. Tout juste peut-on constater que seule une interprétation de l'article 124 de la loi faisant entrer le contenu des communications dans le champ de la confidentialité permettrait de conclure à une transposition cohérente de l'article 5, § 1er de la directive 2002/58/CE « vie privée et communications électroniques »[92].

46. Pour conclure notons que, dans un arrêt du 1er octobre 2009[93], la Cour de cassation a constaté que :

> « En vertu de l'article 124, 1° et 4°, de la loi du 13 juin 2005 relative aux communications électroniques, s'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut prendre intentionnellement connaissance de l'existence d'une information de toute nature transmise par voie de communication électronique et qui ne lui est pas destinée personnellement, ni faire un usage quelconque de l'information obtenue intentionnellement ou non.
> Cet article exclut dès lors notamment la prise de connaissance intentionnelle de l'existence d'un courriel, ainsi que l'usage de cette connaissance ou de l'information qui est ainsi obtenue intentionnellement ou non, par quiconque n'y a pas été autorisé au préalable.
> Quiconque prend connaissance du contenu d'un courriel, ne peut le faire sans prendre connaissance simultanément de son existence. La prise de connaissance et l'usage du contenu d'un courriel sont liés à la prise de connaissance et à l'usage de l'existence de ce courriel. »

---

91 On peut se demander toutefois si les article 109*ter* D de la loi *Télécom* et les articles 314*bis* du Code pénal assuraient une transposition suffisante de la directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications que remplace la directive 2002/58/CE. L'article 5, § 1er de cette directive prévoyait pareillement à son homologue de la directive 2002/58/CE l'obligation pour les États membres de garantir la confidentialité des communications.

92 Voyez en ce sens, C. de Terwangne, J. Herveg et J.-M. Van Gyseghem, *Le divorce et les technologies de l'information et de la communication*, Bruxelles, Kluwer, 2005, p. 50.

93 Cass., 1er octobre 2009, R.G. nº C.08.0064.N, www.cass.be.

Sans fournir une analyse approfondie des termes de la loi, la Cour de cassation constate donc de façon pragmatique que l'article 124 de la loi fait obstacle à la prise de connaissance du contenu de la communication électronique.

c. Qu'implique l'exigence d'un acte intentionnel ?

47. À propos de la notion d'intention, il nous semble que le Tribunal du travail de Bruxelles en fait une application intéressante dans une décision du 4 décembre 2007[94]. Il distingue la découverte fortuite d'un e-mail avec la consultation délibérée d'une telle communication. Ainsi, dans ce litige où l'employeur entendait établir l'existence d'une violation de l'obligation de non-concurrence dans le chef de son travailleur en produisant des e-mails échangés par ce dernier avec des entreprises tierces, le tribunal considéra qu'en l'absence du consentement du travailleur, il appartenait à l'employeur de prouver le caractère fortuit de la découverte des messages produits. Le tribunal constatera que cette preuve n'est pas rapportée, les explications données par l'employeur quant aux circonstances dans lesquelles il a pris connaissance des messages – lors d'un *back up*- n'étant pas convaincantes. Il subodora, compte tenu des tensions qui caractérisaient les relations entre les parties, le fait que l'employeur avait intentionnellement pris connaissance des courriers pour se ménager des preuves dans le cadre de la procédure[95].

48. Dans un jugement rendu le 19 mars 2008, le Tribunal du travail de Liège avait également à trancher si une prise de connaissance d'e-mails pouvait revêtir un caractère fortuit[96].

L'employeur avait licencié une secrétaire après avoir constaté que cette dernière communiquait des informations confidentielles appartenant à l'entreprise à l'ancienne directrice de l'entreprise. Il invoquait avoir été intrigué par un e-mail ouvert visible à l'écran. Cet e-mail se trouvait dans la boîte de messagerie privée Yahoo de la travailleuse. Un coup d'œil indiscret avait permis d'établir qu'il s'agissait d'un message échangé avec l'ancienne directrice. Le Tribunal évoque qu'à cette occasion plusieurs e-mails ont été consultés et imprimés. Le Tribunal estimera que la prise de connaissance initiale des faits est illégale puisqu'elle est le fruit d'une démarche active (consultation et impression d'e-mails) intervenue sans le consentement de la travailleuse.

49. On peut donc retenir de ces décisions qu'il faut faire une distinction entre un contrôle délibéré de l'employeur qui peut se limiter à une démarche

---

94 Trib. trav. Bruxelles (24e ch.), 4 décembre 2007, *J.T.T.*, 2008, p. 179.

95 Pour un commentaire de cette décision voy. K. Rosier, « Régularité de la preuve : tel est pris qui croyait prendre… », *B.S.J.*, 2008, nº 391, p. 5.

96 Trib. trav. Liège, (3e ch.), 19 mars 2008, R.G. nº 360.454, www.cass.be.

de prise de connaissance active d'une communication électronique et la prise de connaissance purement fortuite. Seule la première devrait intervenir en conformité avec les dispositions de la convention collective de travail nº 81 (*cf. infra*, section 5,B du présent chapitre).

d. Durée de la protection

50. Il est généralement admis, sans que cela ne transparaisse clairement du texte, que la protection de l'article 124 est applicable tant pendant la transmission qu'après que la transmission soit achevée. Aussi, la question n'est jamais abordée de front en jurisprudence et en doctrine : il semble aller de soi que la consultation d'un e-mail ayant déjà été ouvert dans la boîte e-mail du travailleur ou d'un *log file* faisant apparaître la liste des sites consultés à partir d'un poste de travailleur tombe sous le coup de l'application de l'article 124.

Une approche sous un angle historique de l'article 124 nous montre toutefois que ceci n'est pas évident.

En effet, la législation actuelle a pour origine la réglementation des télécommunications et était ancrée dans le monde de la téléphonie. L'article 124 remplace l'article 109*ter* D de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques. Cette disposition remplaçait elle-même l'article 111 de cette même loi qui, lui-même était venu remplacer l'article 17 de la loi du 13 octobre 1930 coordonnant les différentes dispositions législatives concernant la télégraphie et la téléphonie avec fil.

51. L'article 17 avait pour objet d'interdire les écoutes téléphoniques. Dans le monde de la téléphonie, le principal enjeu était la saisie d'informations pendant la transmission. Ainsi la doctrine relève-t-elle que certaines décisions de jurisprudence ont considéré que cette disposition emportait l'interdiction d'installer des appareils permettant de collecter des informations relatives à la communication (tels que la date, l'heure, les numéros appelés, etc.)[97]. Ceci étant, aucune de ces dispositions ne contient de précisions concernant la durée de la protection, au contraire des articles 314*bis* et 259*bis* du Code pénal évoqués ci-avant[98]. Les travaux préparatoires ne contiennent pas non plus d'indication à cet égard.

À l'époque de la téléphonie, la question avait essentiellement trait aux données de communication liées à la facturation par exemple et qui restaient disponibles après la fin de la communication sans qu'il y ait eu écoute ou enregistrement par un tiers, tel l'employeur. À cet égard, il n'y avait pas de position tranchée sur la question en doctrine et en jurisprudence. Ainsi, certains

---

97 P. De Hert, « Schending van het (tele)communicatiegeheim in het beroepsleven », *R.D.S.*, 1995, nº 23.

98 *Cf.* Point B, 1, c de la présente section 3, *supra*.

auteurs étaient farouchement opposés à la communication de telles données par les opérateurs téléphoniques à l'employeur[99] tandis que certaines décisions de jurisprudence n'y voyaient aucun obstacle[100].

52. Toujours est-il que c'est sans véritable réflexion à ce sujet, ni état d'âme, que la jurisprudence et la doctrine ont considéré que la protection concernant ces traces laissées par la communication après la transmission achevée comme incluse dans le champ de la protection. En cela, la protection prévue à l'article 124 de la loi sur les communications électroniques se différencie de celle des articles 314*bis* et 259*bis* du Code pénal.

Toutefois, avec l'apparition de nouveau moyens de communication tel l'internet et les courriers électroniques, le champ d'application de la loi de mars 1991 s'est étendu et inclut à présent d'autres formes de communications qui se caractérisent par la rémanence non seulement d'une trace de la communication mais surtout de son contenu. Se pose à présent la question de l'inclusion dans champ d'application de l'article 124 de la loi du 13 juin 2005 du contenu des communications dont nous avons traité *supra*[101].

3. À quelles conditions les actes visés aux articles 314*bis* et 259*bis* du Code pénal ainsi que ceux prévus à l'article 124 de la loi sur les communications électroniques sont-ils autorisés ?

a. Les consentements des personnes concernées par la communication

53. Tant les articles 314*bis*/259*bis* du Code pénal que l'article 124 de la loi du 13 juin 2005 n'érigent en infraction les actes décrits ci-avant que dans l'hypothèse où ils interviennent sans le consentement des parties à la communication.

§ 1er. Quelles sont les personnes dont il convient d'obtenir le consentement ?

54. Les articles 314*bis* et 259*bis* ne posent pas de difficultés particulières. Ils requièrent le consentement des personnes qui sont parties à la communication[102]. Ceci implique les personnes qui prennent part à une communication et ceux qui sont destinataires ou expéditeurs des communications écrites.

---

99 P. De Hert, « Schending van het (tele)communicatiegeheim in het beroepsleven », *R.D.S.*, 1995, nº 36 ; L. Arnou, "Het respecteren van telefoongeheim in België na het afsluiterwet van 30 juni 1994", *Computerrecht* 1995/4, p. 164.

100 Trib. trav. Bruxelles, 16 septembre 2004, R.G. nº 0353058, www.cass.be.

101 *Cf.* Point 2, b, § 3 de la présente section 2.

102 Ceci est d'ailleurs confirmé par les travaux préparatoires aux termes desquels il est précisé qu'une personne à propos de laquelle une conversation est tenue n'est pas à considérée comme une partie à la communication (Projet de loi relatif à la protection de la vie privée contre les écoutes, la prise de

Les termes utilisés dans l'article 124 laissent perplexes. Bien que les termes utilisés soient extrêmement larges et puissent inclure les personnes visées par le contenu de la communication (« S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées… »), la doctrine[103] et la jurisprudence[104] retiennent généralement implicitement que les personnes visées sont les expéditeurs et les destinataires des messages.

§ 2. Quel consentement ?

55. Le consentement doit être libre, spécifique et individuel.

La question du caractère libre se pose avec une acuité particulière dans le cadre d'une relation de travail qui suppose un lien de subordination entre le travailleur et l'employeur. Si le fait de se trouver dans un lien de subordination n'empêche pas *ipso facto* qu'un consentement puisse être librement donné par le travailleur, il convient d'être attentif aux circonstances dans lesquelles il est donné.

Ainsi la Commission de la protection de la vie privée a-t-elle estimé qu'était douteux le caractère libre du consentement de l'employé lorsque celui-ci, pour utiliser internet – à quelque fin, personnelle ou professionnelle, que ce soit, – n'a pas d'autre choix que de cliquer sur le bouton d'acceptation des conditions imposées par l'employeur afin d'avoir accès au réseau[105]. La Cour du travail de Bruxelles a été estimé que le consentement d'une travailleuse obtenu par l'employeur pour consulter certains de ses e-mails lors d'un entretien faisant état du trop grand nombre d'e-mails envoyés par celle-ci depuis son poste à des fins privées ne pouvait être considéré comme libre et éclairé dès lors que la travailleuse se trouvait sous pression au moment où elle avait donné son autorisation. En sens contraire, le Tribunal du travail de Liège

---

connaissance et l'enregistrement de communications et de télécommunications privées, *Doc. Parl.*, Sén., sess. ord. 1992-1993, séance du 1er septembre 1993, p. 843/1, 8).

103 Voy. notamment : J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, p. 85.

104 Pour des décisions concernant l'exigence d'un consentement du travailleur, voy. notamment : C. trav. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262 ; C. trav. Bruxelles, 13 septembre 2005, *Computerr.* 2006, p. 100 ; C. trav. Anvers (sect. d'Anvers), 15 décembre 2004, *Chron. D.S.*, 2006, p. 146 ; C. trav. Bruxelles (3e ch.), 10 février 2004, *Oriëntatie*, 2004, p. 3, note A Vanoppen ; *Orientations*, 2006, p. 141 ; C. trav. Anvers (sect. Anvers), 1er octobre 2003, *J.T.T.*, 2004, p. 510 ; Trib. trav. Hasselt (1re ch.) 21 octobre 2002, *Chron. D.S.*, 2004, p. 197.

105 Commission de la protection de la vie privée, Avis nº 13/03 sur le contrôle par l'employeur des données de communication de l'un de ses employés, 27 février 2003, p. 5, www.privacycommission.be.

a estimé qu'une travailleuse confrontée à une demande de consultation de ses e-mails en présence d'un huissier pouvait valablement y consentir[106].

56. Qu'en est-il d'un possible consentement donné *a priori* sur le principe du contrôle lui-même ?

Le caractère spécifique du consentement peut faire obstacle à ce que celui-ci soit donné anticipativement et de manière générale. Dans les travaux préparatoires de la loi du 30 juin 1994 insérant les articles 314*bis* et 259*bis* du Code pénal, il est d'ailleurs spécifié qu'une clause par laquelle un employeur se réserverait le droit d'écouter des conversations téléphoniques de son employé serait inacceptable[107]. Il résulte de ces considérations qu'un consentement obtenu de manière générale par l'employeur ne serait pas suffisant. Face à cette exigence de spécificité, il est apparu nécessaire à certains auteurs de préciser que le consentement pour la prise de connaissance des communications n'implique pas nécessairement un consentement pour l'enregistrement ou la conservation de celles-ci.

57. Le consentement doit encore être individuel. À cet égard, si l'insertion au sein du règlement de travail de règles relatives à l'utilisation de l'e-mail ou de l'internet est parfaitement envisageable, reste la question de savoir si on peut y inscrire le principe d'une autorisation de l'employé donnée à l'employeur de consulter ses e-mails.

58. On peut encore se demander si le consentement doit être explicite ou s'il peut être tacite. Les travaux préparatoires de la loi du 30 juin 1994 insérant les articles 314*bis* et 259*bis* du Code pénal n'excluent pas cette dernière possibilité[108]. La doctrine a relevé qu'il a été considéré qu'il y avait consentement tacite mais indubitable lorsqu'une conversation est menée par le biais d'une technologie impliquant que l'écoute de la conversation puisse avoir lieu

---

106 Elle a toutefois estimé qu'en l'espèce, dès lors que cette demande était formulée parce que l'employeur avait constaté initialement des faits au moyen d'une consultation illicite et au mépris total du principe de loyauté dans l'exécution du contrat de travail, l'irrégularité initiale implique que toutes les démarches ultérieures visant à obtenir une preuve de ces faits sont entachées d'irrégularité. (Trib. trav. Liège [3e ch.], 19 mars 2008, R.G. nº 360.454, www.cass.be). Sur ce point, le tribunal rejoint la position adoptée par le Tribunal du travail de Bruxelles dans un jugement du 4 décembre 2007 qui avait considéré qu'« il ne saurait par ailleurs être recouru à d'autres modes de preuve, tels des enquêtes, pour établir des éléments révélés par ces preuves acquises illégalement » (Trib. trav. Bruxelles [24e ch.], 4 décembre 2007, *J.T.T.*, 2008, p. 179).

107 Projet de loi relatif 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. ord. 1992-1993, séance du 1er septembre 1993, p. 843/1, 8.

108 Projet de loi relatif 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. ord. 1992-1993, séance du 1er septembre 1993, p. 843/1, 8 et p. 843/2, 10.

ou dans l'hypothèse où une secrétaire devait noter ce qui était dit lors d'une conversation téléphonique[109]. La Cour du travail d'Anvers a estimé, entre autres considérations, que le fait que la travailleuse licenciée pour avoir fait un usage intensif de l'e-mail à des fins privées avait communiqué à son collègue son mot de passe emportait son consentement implicite pour que ce dernier consulte ses e-mails[110]. Ceci étant, on relèvera avec F. Hendrickx, qu'il ne suffit pas toutefois que la conversation ait lieu dans un cadre professionnel pour pouvoir en déduire l'existence d'un consentement[111]. Là encore, il y a lieu d'apprécier au cas par cas.

On le voit, la question du consentement reste délicate tandis que nombre de décisions de jurisprudence insistent sur le fait que des données électroniques ne peuvent être produites sans *le consentement* du travailleur et/ou les autres parties à la communication et, à défaut, ont déclaré la preuve irrecevable[112].

59. La Commission de la protection de la vie privée a préconisé que le consentement du travailleur soit sollicité par rapport à des modalités de contrôle négociées collectivement. En effet, elle considère, dans sa recommandation n° 1/2002 du 22 août 2002[113] que, « En ce qui concerne les employés, une note de service ou le règlement de travail seul 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'enregistrements 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 ».

Si cette approche peut offrir une solution pour le contrôle des connexions à l'internet des travailleurs y ayant consenti dans la mesure où celles-ci n'impliquent aucune communication avec un tiers ou des e-mails ou autres com-

---

109 L. Arnou, « Uit respecteren van het telefoon geheim in België na de afsluiterwet van 30 juni 1994 », *Computerrecht*, 1995/4, p. 160.

110 C. trav. Anvers (section d'Anvers), 8 janvier 2003, R.G. n° 2020255, www.cass.be.

111 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 197.

112 C. trav. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262 ; C. trav. Bruxelles, 13 septembre 2005, *Computerrecht*, 2006, p. 100 ; C. trav. Anvers (section d'Anvers), 15 décembre 2004, R.G. n° 2004-0295, www.cass.be, C. trav. Bruxelles (3e ch.), 10 février 2004, *Oriëntatie*, 2004, p. 3, note A Vanoppen, *Orientations*, 2006, p. 141 ; C. trav. Anvers (section Anvers), 1er octobre 2003, *J.T.T.*, 2004, p. 510 ; Trib. trav. Hasselt (1re ch.) 21 octobre 2002, *Chron. D.S.*, 2004, p. 197 ; C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2001, p. 41 ; Trib. trav. Bruxelles (12e ch.), 22 juin 2000, *Computerrecht*, 2001/6, p. 312.

113 Commission de la protection de la vie privée, Recommandation n° 01/2002 relative à l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, 22 août 2002, www.privacycommission.be.

munications électroniques entre personnes ayant accepté le contrôle, il demeure qu'elle reste imparfaite en ce qui concerne les communications impliquant des tiers. Certes, la transparence et la prévisibilité d'une solution négociée est de nature à désamorcer certains conflits mais il demeure qu'aux termes de la loi, le consentement de toutes les parties concernées est requis[114]. Si l'on peut concevoir d'obtenir le consentement de l'employé partie à la communication, qu'en est-il du tiers qui, en qualité de destinataire ou d'expéditeur, est partie à la communication ? L'exigence d'un consentement véritable interdit d'envisager de se limiter à informer les destinataires de courriers électroniques du fait que tous les e-mails adressés par l'employé sont susceptibles d'être lus ou conservés par l'employeur. D'où la question cruciale : un employeur pourrait-il se prévaloir de l'une ou l'autre exception prévue à l'article 125 pour opérer un contrôle sans le consentement des parties concernées par la communication.

b. Les exceptions prévues à l'article 125 de la loi

60. L'article 125 de la loi prévoit des exceptions à ces interdictions dans les hypothèses suivantes :

> « 1° lorsque la loi permet ou impose l'accomplissement des actes visés ;
> 2° lorsque les actes visés sont accomplis dans le but exclusif de vérifier le bon fonctionnement du réseau et d'assurer la bonne exécution d'un service de communications électroniques ;
> 3° lorsque les actes sont accomplis en vue de permettre l'intervention des services de secours et d'urgence en réponse aux demandes d'aide qui leur sont adressées ;
> 4° lorsque les actes sont accomplis par l'Institut dans le cadre de sa mission générale de surveillance et de contrôle ;
> 5° lorsque les actes sont accomplis par le service de médiation pour les télécommunications ou à la demande de celui-ci dans le cadre de ses missions légales de recherche ;
> 6° lorsque les actes sont accomplis dans le seul but d'offrir des services à l'utilisateur final consistant à empêcher la réception de communications électroniques non souhaitées, à condition d'avoir reçu l'autorisation de l'utilisateur final à cet effet ».

61. Si l'on se place dans la perspective de permettre à l'employeur de prendre connaissance des e-mails échangés par ses employés, dans le cadre d'un contrôle ponctuel par exemple, seules les deux premières hypothèses recèlent potentiellement un intérêt.

---

114 C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2001, p. 41.

La seconde exception ne permet toutefois que l'accomplissement de mesures d'ordre strictement technique. Certains auteurs[115] ont fait remarquer, à propos de la même exception qui était déjà prévue à l'article 109*ter* E, § 1er, 1°, que celle-ci vise en réalité des interventions sur le réseau public de communications, et ce en se fondant sur les travaux préparatoires de la loi[116]. Interpellé sur ce qu'il adviendrait dans l'hypothèse où l'employé d'un opérateur effectuerait d'initiative des écoutes téléphoniques – le libellé de la disposition tel que proposé évoquait *les actes visés posés pour assurer un service de télécommunication* –, le ministre de l'époque avait précisé qu'étaient visés les actes *ayant pour but* d'assurer ledit service. Certains auteurs en déduisirent que n'étaient concernés que les actes assurant la fourniture d'un service sur un réseau public, ce qui nous paraît discutable. D'autres auteurs ont d'ailleurs interprété l'exception dont question comme permettant des interventions nécessitées sur le réseau de l'entreprise[117].

62. Quoi qu'il en soit, il n'empêche que l'accomplissement de ces actes pourrait donner lieu à une prise de connaissance fortuite d'une communication problématique.

C'est ainsi que, dans une décision du 4 décembre 2007, le Tribunal du travail de Bruxelles[118] relève que, en l'absence du consentement du travailleur, il appartient à l'employeur de prouver le caractère fortuit de la découverte des messages produits. Ce faisant, le tribunal admet que, dans l'hypothèse où l'employeur peut démontrer que la prise de connaissance des informations est fortuite et non intentionnelle, la preuve pourrait être recevable. En l'espèce, l'employeur invoquait que les e-mails avaient été découverts lors d'un *back up*. Le Tribunal considèrera toutefois que la preuve des circonstances dans lesquelles les e-mails avaient été découverts n'était pas démontrée.

63. Mise à part l'hypothèse d'une intervention technique sur le réseau, la prise de connaissance des données ou du contenu de la communication ne peut se faire que dans le cas où une loi le permet ou l'impose.

---

115 J. Dumortier, « internet op het werk, controlerechten van de werkgever », *Or.*, 2000, p. 38 ; Th. Claeys et D. Dejonghe, « Gebruik van *e-mail* en internet op de werkplaats en controle door de werkgever », *J.T.T.*, 2001, p. 128.

116 Projet de loi portant réforme de certaines entreprises publiques économiques, *Doc. Parl.*, Ch. repr., session 1990-1991, nº 1287/10-89/90, p. 174.

117 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, nº 35, pp. 51-52 ; H. Barth, « Contrôle de l'employeur de l'utilisation « privée » que font ses travailleurs des nouvelles technologies de l'information et de la communication au lieu de travail », *J.T.T.*, 2002, p. 173.

118 Trib. trav. Bruxelles (24e ch.), 4 décembre 2007, *J.T.T.*, 2008, p. 179.

S'agit-il d'une loi au sens formel ? Ni la loi, ni les travaux préparatoires n'en disent mot. Si l'on a égard à l'article 22 de la Constitution, il nous semble toutefois qu'il faille répondre par l'affirmative. En effet, dès lors que cette disposition réserve au législateur seul le droit de restreindre le droit à la protection de la vie privée et qu'une exception à l'article 124 induit assurément une telle atteinte, il nous faut en déduire que seul un texte de valeur législative est susceptible de pouvoir éventuellement prévoir ou permettre l'accomplissement des actes en question.

64. La question se pose de savoir si la loi du 3 juillet 1978, et en particulier les articles de la loi consacrant le pouvoir d'autorité de l'employeur peuvent constituer une base légale suffisante au regard de l'article 109*ter* E de la loi *Belgacom* et de la disposition qui y a été substituée, l'article 125 de la loi du 13 juin 2005. Selon F. Hendrickx, l'article 17, 2° de la loi sur le contrat de travail ne peut offrir une base suffisante à des atteintes à la vie privée qu'en ce qui concerne l'exercice normal de l'autorité patronale[119]. Il semble d'ailleurs se dégager une opinion majoritaire pour rejeter l'idée que ces dispositions auraient un caractère suffisamment précis que pour constituer une base légale adéquate[120]. La Commission de la protection de la vie privée a elle aussi fait sienne cette position en constatant que « la surveillance électronique des travailleurs ne peut pas être assimilée sans plus à une forme "moderne" d'exercice de l'autorité »[121].

En sens contraire, M. Lauvaux, V. Simon et D. Stas de Richelle relèvent toutefois que, dans le cadre de l'examen de l'article 314*bis* du Code pénal, le Tribunal du travail de Bruxelles[122] et la Cour du travail de Gand[123] ont

---

119 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 61.

120 Comme le constatent J.-P. Cordier et S. Bechet (J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008) et O. Rijckaert (O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n° 35, p. 51). Ainsi, selon F. Hendrickx, l'article 17, 2° de la loi sur le contrat de travail n'offre aucune base suffisamment précise et claire pour en déduire la possibilité d'utiliser des caméras de surveillance, de procéder à des examens médicaux ou à des écoutes téléphoniques ou encore à la fouille de membres du personnel ou de toute autre atteinte du même ordre (F. Hendrickx, *Electronisch toezicht op het werk, internet en camera's*, Ced. Samson, 2001, p. 308) ; voy. également : J. Dumortier, « internet op het werk, controlerechten van de werkgever », *Oriëntatie*, 2000 p. 38 ; P. Leduc, « Le contrôle des communications données et reçues par le travailleur », *Revue Ubiquité*, 2000/5, p. 47 ; J.-P. Lacomble et C. Preumont, « Ontslag wegens dringende reden en bescherming van privacy », *Cah. Jur.*, 2005, p. 96 ; C. trav. Bruxelles (3e ch.), 8 avril 2003, *Chron. D.S.*, 2005, p. 208 ; *contra* : R. De corte, « Surfen op het werk : een kwestie van niet uitglijden », *De juristenkrant*, 7 nov. 2000, p. 7 et F. Lagasse, « La vie privée et le droit du travail », *Chron. D.S.*, 1997, p. 425.

121 Commission de la protection de la vie privée, Avis n° 13/03 sur le contrôle par l'employeur des données de communication de l'un de ses employés, 27 février 2003, p. 9, www.privacycommission.be.

122 Trib. trav. Bruxelles, 16 septembre 2004, *J.T.T.*, 2005, p. 61.

123 C. trav. Gand, 9 mai 2005, R.G. n° 269/02, ww.cass.be.

estimé ces articles suffisants pour autoriser une ingérence de l'employeur dans la vie privée du travailleur[124]. Nous avons également relevé des décisions qui se prononcent expressément en ce sens à propos de l'article 109*ter* D[125].

65. Épinglons encore ces décisions du Tribunal du travail de Bruxelles qui a estimé que l'application de l'article 16 de la loi du 3 juillet 1978 en ce qu'il impose à l'employeur d'assurer le respect des convenances et des bonnes mœurs sur le lieu de travail, constitue une « autorisation légale » d'exercer un contrôle[126]. O. Rijckaert souscrit à ce point de vue en indiquant que « ne pas admettre que, dans des circonstances d'une gravité exceptionnelle, l'employeur puisse intervenir en prenant connaissance du contenu d'un e-mail, reviendrait à lui dénier la possibilité de respecter, entre autres, son obligation légale de garantir le respect des bonnes mœurs sur le lieu de travail »[127].

c. Les exceptions prévues à l'article 128 de la loi du 13 juin 2005 sur les communications électroniques

§ 1er. L'enregistrement de communications commerciales

66. L'article 128, § 1 de loi du 13 juin 2005 relative aux communications électroniques prévoit la possibilité d'enregistrer une communication électronique dès lors que celle-ci est effectuée dans le cadre de transactions commerciales licites et que l'enregistrement intervient dans le but de faire la preuve d'une transaction commerciale ou d'une autre communication professionnelle. Cet enregistrement est toutefois soumis à des exigences strictes : toutes les parties impliquées dans la communication doivent avoir été préalablement informées de l'enregistrement, des objectifs précis de ce dernier ainsi que de la durée de stockage de l'enregistrement. De plus, les données visées dans cette disposition doivent être effacées au plus tard à la fin de la période pendant laquelle la transaction peut être contestée en justice. Enfin, l'article 128 précise que la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel reste applicable aux traitements de données à caractère personnel qu'implique cet enregistrement.

67. Il paraît extrêmement difficile d'assurer une information préalable de toutes les personnes concernées sachant que dans nombre de cas le courrier électronique que l'entreprise souhaitera conserver lui sera adressé par un tiers

---

124 M. Lauvaux, V. Simon et D. Stas de Richelle, *Criminalité au travail*, Bruxelles, Kluwer, 2007, p. 102.

125 C. trav. Mons, 25 novembre 2009, *R.D.T.I.*, 2009, p. 229, note K. Rosier et S. Gilson.

126 Trib. trav. Bruxelles (12e ch.), 22 juin 2000, *Computerrecht*, 2001/6, p. 11 ; Trib. trav. Bruxelles, 6 septembre 2001, *J.T.T.*, 2002, p. 52.

127 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, nº 35, p. 51.

sans qu'elle ait pu l'informer quant à sa politique d'enregistrement des courriers électroniques. Par ailleurs, l'autorisation du seul enregistrement peut être insuffisante si la prise de connaissance n'est pas autorisée également. Enfin, la conciliation de cette disposition avec la loi du 8 décembre 1992 suscite également des questions. Par exemple, le libellé de l'article 128 n'indique pas clairement si l'obligation d'information de l'article 9 de la loi du décembre 1992 reste applicable ou si elle est remplacée par celle décrite dans la disposition.

L'article 128, § 1 paraît donc plus adapté à l'enregistrement systématique de courriers électroniques dans le cadre d'une activité bancaire, par exemple, où les utilisateurs d'un service bancaire à distance sont prévenus que les communications électroniques échangées avec la banque seront automatiquement enregistrées. En revanche, son application dans l'ensemble du secteur commercial et professionnel de manière plus générale, comme le suggère son texte, nous paraît problématique.

§ 2. L'enregistrement de communications téléphoniques dans le cadre de *call center*

68. L'article 128, § 2 de la loi du 13 juin 2005 crée une seconde dérogation aux articles 259*bis* et 314*bis* du Code pénal en admettant la prise de connaissance et l'enregistrement de communications électroniques et des données de trafic, qui visent uniquement à contrôler la qualité du service dans les *call center* moyennant respect de certaines conditions.

Si cette disposition fait tomber l'exigence de l'obtention du consentement préalable de toutes les parties, elle maintient toutefois que les personnes qui travaillent dans le *call center* doivent être informées au préalable du but précis de cette opération, de la possibilité de prise de connaissance et d'enregistrement et de la durée de conservation de la communication qui ne peut excéder un mois. L'article 128, § 2 indique expressément que ceci est sans préjudice de l'application de la loi du 8 décembre 1992 relative à la protection de la vie privée.

d. L'état de nécessité

69. F. Hendrickx a évoqué la possibilité de se prévaloir de l'état de nécessité pour poser des actes en principe prohibés sous le couvert du secret des communications électroniques[128]. Il s'agirait de justifier *a posteriori* le non-respect de ces dispositions par cette cause générale de justification en droit pénal. Comme le rappelle O. Rijckaert, seules des situations extrêmes pourraient éventuellement permettre l'invocation de cette cause de justification et l'auteur de citer

[128] F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, pp. 199-200.

la commission par le travailleur d'une infraction d'une gravité extrême (telle la réception ou la distribution d'images pédophiles ou la divulgation de secrets de fabrique)[129].

4. Qu'en est-il de la pratique du « *forward* » ?

70. Si on s'en tient au prescrit de l'article 124 de la loi du 13 juin 2005, un tiers à la communication ne peut prendre connaissance des données s'il n'y est pas autorisé par toutes les personnes qui y sont parties. C'est en ce sens que la Cour du travail de Bruxelles a écarté des débats des courriers électroniques et SMS versés par l'employeur pour établir des faits de harcèlement sexuel dans le chef de l'employé licencié dès lors que ceux-ci avaient été obtenus sans le consentement de l'employé et donc en violation de l'article 109*ter* D, 3° de la loi du 21 mars 1991[130]. Dans le cas d'espèce, il est intéressant de relever que la Cour ne s'interroge pas sur la manière dont les SMS se sont trouvés en possession de l'employeur alors qu'il est vraisemblable, compte tenu des faits de la cause, que ce soit la collègue victime du harcèlement et destinataire des SMS qui les ait communiqués à son employeur. La Cour semble donc considérer que le simple fait que l'employeur soit tiers à la communication suffit à l'obliger, au regard de l'article 109*ter* D, à obtenir le consentement de toutes les parties à la communication.

Notons que le Tribunal du travail de Liège parvient à une toute autre conclusion à propos d'un e-mail communiqué dans des circonstances comparables[131]. Il estime que dès lors que la personne est régulièrement entrée en possession du message, elle est en droit de le transmettre à son employeur. Le Tribunal considère que le fait d'être le destinataire d'un message implique qu'on l'a obtenue de manière régulière. Cette conclusion se base sur le fait que la preuve a été ou non obtenue loyalement mais fait fi du fait qu'elle a ou non été obtenue de manière licite, c'est-à-dire sans violation de la loi.

71. On pourrait toutefois se demander si dans ce cas, on doit considérer que la prise de connaissance est intentionnelle, élément déterminant dans l'application de l'article 124. Dans l'hypothèse d'un transfert d'e-mail, le destinataire reçoit des informations sans les avoir activement recherchées. Or, comme évoqué sous le point B, 2, c de la présente section, *supra*, on dénote en jurispru-

---

129 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, 2005, n° 35, p. 52.

130 C. trav. Bruxelles (3e ch.), 10 février 2004, *Oriëntatie*, 2004, p. 3, note A. Vanoppen ; *Orientations*, 2006, p. 141.

131 C. trav. Liège (section Namur), 23 mars 2004, R.G. n° 7387-03, www.cass.be.

dence une tendance à opposer au caractère intentionnel de la prise de connaissance, le caractère fortuit, involontaire de celle-ci[132].

Le non-respect du secret des communications ne se situerait plus sur le terrain du secret des communications électroniques mais sur celui du secret de la correspondance issu de l'article 8 de la C.E.D.H. et sur lequel nous reviendrons[133]. Cette méconnaissance de la confidentialité du message serait imputable à la personne partie à la communication initiale qui aurait transmis des informations éventuellement confidentielles au mépris de ce droit.

5. Conclusion

72. Dans l'état actuel de la législation, il est donc interdit de prendre connaissance intentionnellement de *données en matière de communications électroniques* relatives à une autre personne ou de révéler, de faire un usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non sauf moyennant l'autorisation de toutes les parties à la communication. Ainsi, la simple consultation d'une boîte e-mail pour vérifier à qui une personne a adressé des e-mails, à quelle date, etc. sans même ouvrir le courrier électronique est prohibée.

Les dispositions précitées qui assurent la transposition de l'article 5, § 1er de la directive « vie privée et communications électroniques » sont essentiellement inspirées par les risques spécifiques liés aux nouvelles technologies et qui permettent à une personne de prendre connaissance à distance d'informations qui ne lui sont pas destinées[134]. On doit même constater que l'aspect technologique induit en fin de compte une protection plus forte que pour la correspondance échangée hors réseau.

73. On peut, de fait, voir une certaine discordance entre le régime d'« interception » des courriers papiers et celui des e-mails.[135] En effet, le secret des lettres et de la correspondance est consacré par les articles 29 de la Constitution

---

132 C. trav. Bruxelles (4e ch.), 28 novembre 2006, *Chron. D.S.*, 2009, p. 3 ; Trib. trav. Bruxelles (24e ch.), 4 décembre 2007, *J.T.T.*, 2008, p. 179 ; Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. nº 360.454, www.cass.be ; C. trav. Bruxelles, 8 avril 2003, *Chron. D.S.*, 2005, p. 208 ; C. trav. Anvers (section Hasselt), 15 novembre 2005, *Chron. D.S.*, 2006, p. 153.

133 *Cf.* point B, 5 de la présente section.

134 Ainsi le considérant 21 de la directive 2002/58/CE « vie privée et communications électroniques » précise-t-il : « Il convient de prendre des mesures pour empêcher tout accès non autorisé aux communications afin de protéger la confidentialité des communications effectuées au moyen de réseaux publics de communications et de services de communications électroniques accessibles au public, y compris de leur contenu et de toute donnée afférente à ces communications ».

135 À cet égard, voy. R. Robert, « Correspondance et vie privée sur les lieux de travail : une cohabitation difficile », *Orientations*, 2008, pp. 16-22.

et 460 du Code pénal. Son champ d'application est sensiblement différent du régime de protection des communications électroniques.

Cette protection exclut le fait de prendre ou d'ouvrir des lettres et de porter atteinte à leur caractère confidentiel[136]. Ainsi, selon F. Hendrickx, la protection constitutionnelle du secret des lettres vaut également entre particuliers et s'applique à la correspondance que l'on reçoit sur le lieu du travail[137]. Cette position concernant le caractère privé des correspondances professionnelles ne fait toutefois pas l'unanimité[138]. En toute hypothèse, ce secret ne s'oppose pas, nous semble-t-il à ce qu'une fois ouvert, le courrier qui fait partie d'une correspondance professionnelle puisse être consulté par l'employeur sans le consentement du tiers et même sans le consentement de l'employé tandis que les articles 124 et 125 de la loi du 13 juin 2005 ne le permettent pas en ce qui concerne les communications électroniques, même professionnelles[139]. C'est ainsi que la Cour du travail de Liège a considéré « qu'il convient d'opérer une distinction entre ce qui ressort du strict domaine de la vie privée sur le lieu du travail, qui est protégé et ce qui est ou devrait être du ressort de l'exercice de l'activité professionnelle, qui ne l'est pas. Ainsi, un employeur est en droit de contrôler le courrier entrant (sauf adressé en nom personnel à l'employé) et sortant (aux frais de l'entreprise) parce qu'il revêt en principe un caractère professionnel »[140]. En outre, la Cour du travail de Liège a jugé que par correspondance, il faut entendre « échange épistolaire confié à la poste ou à un organisme chargé de la distribution du courrier ; que le principe de l'inviolabilité des lettres vaut à l'égard du pouvoir mais une fois la lettre remise à sa destination, ce sont les principes du droit privé qui garantissent le secret

---

136 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 207 ; voy. également : J.-P. Cordier et S. Bechet, « La preuve du motif grave et les règles relatives à la protection de la vie privée : conflit de droits ? », *in* S. Gilson (coord.), *Quelques propos sur la rupture du contrat de travail. Hommage à P. Blondiau*, Louvain-la-Neuve, Anthemis, 2008, p. 109.

137 L'auteur s'en réfère, à ce titre, à une réponse qui a été faite devant le Sénat par Cardoen dans *Réponse Sénat*, 1987-1988, 4, n° 1 (F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 206) ; dans le même sens P. De Hert, « Schending van het (tele)communicatiegeheim in het beroepsleven », *R.D.S.*, 1995, pp. 266 et 267.

138 *Contra* : J.-M. Leboutte, « De wettelijke bescherming van het briefgeheim », *De Gemeente*, 1988, p. 370 ; F. Lagasse et M. Milde, « Protection de la personne et vie privée du travailleur. Investigation et contrôle sur les lieux du travail », *Orientations*, 1992, p. 153.

139 C'est donc à tort, selon nous, que les partenaires sociaux ont affirmé au sein de la convention collective de travail n° 81 que « lorsque l'objet et le contenu des données de communications électroniques en réseau ont un caractère professionnel non contesté par le travailleur, l'employeur pourra les consulter sans autre procédure. Le bon fonctionnement de l'entreprise doit être assuré » (C.C.T. n° 81 du 26 avril 2002 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau, rendu obligatoire par arrêté royal du 21 juin 2002, *M.B.*, 29 juin 2002).

140 C. trav. Liège (sect. Namur), 25 avril 2002, R.G. n° 6.520/99, www.cass.be.

des correspondances vis-à-vis des citoyens entre eux »[141]. La Cour reconnaît donc une protection par les articles 22 de la Constitution et 8 de la C.E.D.H. une fois la lettre remise à destination. On peut voir dans le régime du secret des lettres plus de souplesse et de flexibilité pour permettre l'ouverture et la prise de connaissance des lettres par l'employeur[142]. Cette discordance avec le régime des communications électroniques ne fait qu'ajouter à la complexité du régime de protection de la vie privée des individus sur leur lieu de travail.

74. Le régime concernant les communications électroniques revient donc à empêcher toute prise de connaissance d'un courrier électronique adressé à un travailleur même si ce dernier reconnaît le caractère professionnel de l'e-mail. Comment concilier cette protection quasi-absolue avec l'encouragement que les dispositions légales entendent donner au développement de l'utilisation de cette technologie ? À l'heure où le législateur a consacré l'équivalence fonctionnelle entre écrit papier et écrit sur support électronique[143] et permet la signature électronique, comment justifier cette protection aveugle du courrier électronique professionnel ?

On ne peut que regretter à cet égard que la transposition de la directive 2002/58/CE « vie privée et communications électroniques » n'ait pas été l'occasion d'une véritable réflexion sur la question.

Si le législateur a inséré un article 128 dans la loi du 13 juin 2005 destiné à permettre l'enregistrement de communications électroniques par l'employeur, la portée restreinte que lui confèrent les conditions posées et les actes permis par cette disposition la prive presque de toute utilité pratique.

L'intervention du législateur pour définir un cadre légal dans cet imbroglio juridique serait la bienvenue. Nous n'avons toutefois pas connaissance de projets allant dans ce sens. Le vice-président de la Commission de la protection de la vie privée annonçait dans le cadre d'un colloque du 18 novembre 2010 que la Commission envisageait d'émettre des recommandations sur la question qui devraient proposer de nouvelles balises pour l'interprétation des normes en vigueur[144].

---

141 *Ibidem.*

142 La Cour de cassation française a d'ailleurs fait cette curieuse distinction entre ouverture de courrier et prise de connaissance dans son arrêt nº 251 du 18 mai 2007, accessible sur www.courdecassation.fr ; pour de plus amples développements, voy. R. Robert, « Correspondance et vie privée sur les lieux de travail : une cohabitation difficile », *Orientations*, 2008, p. 16.

143 En vertu de l'article 16, § 2 de la loi du 11 mars 2003 relative à certains aspects juridiques des services de la société de l'information, il y a lieu de considérer que l'exigence d'un écrit est satisfaite par une suite de signes intelligibles et accessibles pour être consultés ultérieurement, quels que soient leur support et leurs modalités de transmission.

144 Colloque « Vie privée au travail » organisé à Louvain-la-Neuve le 18 novembre 2010 par l'U.C.L. À l'heure où les auteurs terminent le présent texte, cet avis n'est pas encore rendu public.

C. Le traitement des données relatives au trafic et à la localisation

75. L'utilisation de données de localisation s'est considérablement développée depuis ces dernières années, avec l'apparition de nouvelles applications et technologies permettant d'obtenir des informations sur la localisation des personnes.

Le grand succès du GPS (*Global Positioning System*) a évidemment contribué à la multiplication des possibilités de localiser une personne via un terminal tel qu'un navigateur GPS par exemple. L'utilisation de nouvelles applications comme Google Latitude (service de Google qui permet de localiser un individu sur une carte grâce à son téléphone portable) rend possible également le fait de tracer des individus dans leurs déplacements. Ces services ne sont donc plus fondés sur la localisation d'un individu à sa demande, mais peuvent également permettre une localisation à la demande d'un tiers (en l'occurrence, l'employeur)[145].

S'est alors posé le problème de savoir comment ces données allaient être traitées, sachant qu'elles font l'objet d'une attention particulière dans les dispositions de la loi du 13 juin 2005 transposant en droit belge la Directive 2002/58/CE « vie privée et communications électroniques ».

76. Pour les besoins de la législation applicable aux fournisseurs de services de communications électroniques (tels les fournisseurs d'accès à internet ou les fournisseurs de services de téléphonie), la loi du 13 juin 2005 définit deux types de données générées lors des communications.

Il s'agit, d'une part, des données de trafic et, d'autre part, des données de localisation.

Par « donnée de trafic », on entend « toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communication électronique ou de la facturation de ce type de communication »[146]. Certaines de ces données de trafic sont en outre des données de localisation c'est-à-dire des « données traitées dans un réseau de communication électronique indiquant la position géographique de l'équipement terminal d'un utilisateur final d'un service de communication électronique accessible au public »[147].

---

145 Plusieurs objectifs peuvent être poursuivis par l'employeur. Ainsi, le contrôle peut avoir pour but de vérifier si les pauses sont trop longues, si le travailleur a commencé à l'heure, s'il a emprunté le chemin le plus court, à quelle vitesse il a roulé, si le véhicule a été utilisé pendant le week-end, si les rapports de clientèle ont été correctement établis ; voy. A. Peiffer, A. Matthijs, et E. Verlinden, « iPrivacy in de arbeidsrelatie », Story Publishers, Gent, 2008, p. 121.

146 Art. 2, 5° de la loi du 13 juin 2005 relative aux communications électroniques.

147 Art. 2, 6° de la loi du 13 juin 2005 relative aux communications électroniques.

Lorsqu'un employeur souhaite qu'un fournisseur de services de communication lui permette d'obtenir des données indiquant la position géographique d'un utilisateur, entrent donc en jeu des données de localisation.

Or, le traitement de données de localisation, dans le cadre de la fourniture d'un service de communication[148], est soumis à certaines conditions. Dès lors qu'un fournisseur de communication (tel un fournisseur d'accès internet ou un opérateur de téléphonie) inclut dans son service la possibilité d'un service recourant à la localisation de l'utilisateur, il est soumis à certaines obligations. Ainsi, pour fournir un service à données de localisation, c'est-à-dire, un service qui exige un traitement particulier des données de localisation allant au-delà de ce qui est strictement nécessaire pour la transmission ou la facturation de la communication[149], le fournisseur doit obtenir le consentement libre et informé de l'abonné ou, le cas échéant, de l'utilisateur final[150], et respecter les dispositions applicables de la loi du 8 décembre 1992 dont il sera question dans la section *infra*.

77. Remarquons toutefois que toute géolocalisation ne tombera pas forcément sous le coup de l'application de la loi du 13 juin 2005. Comme l'a fait remarquer la Commission de la protection de la vie privée[151], il se peut que le service fourni le soit par un tiers qui n'est pas un fournisseur de services de communications électroniques. La Commission cite l'exemple de GSM proposés actuellement sur le marché et combinés à un système GPS. Ce type de GSM traite des données de localisation qui pourraient être communiquées directement via un tiers, non fournisseur de services à données de localisation. Ce dernier ne serait pas tenu par les obligations définies dans la loi du 13 juin 2005. La seule loi applicable serait la loi du 8 décembre 1992 .

---

148 Le terme « service de communication » vise le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission, en ce compris les opérations de commutation et de routage, de signaux sur des réseaux de communications électroniques, à l'exception (a) des services consistant à fournir un contenu (à l'aide de réseaux et de services de communications électroniques) ou à exercer une responsabilité éditoriale sur ce contenu, à l'exception (b) des services de la société de l'information tels que définis à l'article 2 de loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et à l'exception (c) des services de la radiodiffusion y compris la télévision (art. 2, 5° de la loi du 13 juin 2005 relative aux communications électroniques). Cela concerne typiquement la fourniture d'un accès internet ou des services de téléphonie.

149 Art. 2, 9° de la loi du 13 juin 2005 relative aux communications électroniques.

150 Art. 123, § 2 de la loi du 13 juin 2005 relative aux communications électroniques.

151 Commission de la protection de la vie privée, Avis n° 18/2007 sur une proposition de loi modifiant la loi relative aux communications électroniques en vue d'assurer une meilleure protection de la vie privée pour les "services à données de localisation" ou services de "géolocalisation" par téléphone portable, 27 avril 2007, p. 4, www.privacycommission.be.

Il en est de même pour les équipements de localisation utilisant les systèmes GPS ou GPRS. Dans cette hypothèse, le fournisseur de l'équipement et du service n'est généralement pas un fournisseur de service de communications électroniques.

Section 4
La protection des données à caractère personnel : une législation d'application transversale

78. Il convient encore de tenir compte d'une loi d'application transversale : la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel.

Le législateur européen n'a, jusqu'à présent, pas adopté de directive européenne spécifique aux traitements de données dans le cadre de la relation de travail. Une réflexion est cependant en cours concernant l'opportunité d'adopter une directive spécifique au traitement de données à caractère personnel dans le contexte professionnel. C'est dans ce cadre que le Groupe de l'Article 29[152] avait rendu un avis sur la question[153] et que la Commission avait lancé une procédure de consultation des partenaires sociaux[154].

Au niveau européen, le siège de la matière est donc le droit commun de celle-ci, à savoir la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la circulation des données[155] et la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[156].

79. Cette loi de portée générale s'applique pleinement dans le contexte professionnel[157].

---

152 Il s'agit d'un organe consultatif européen indépendant sur la protection des données et de la vie privée, établi en vertu de l'article 29 de la directive 95/46/CE.

153 Groupe de l'Article 29, Avis 8/2001, du 13 septembre 2001 sur le traitement de données à caractère personnel dans le contexte professionnel, 5062/01, WP 48, p. 4.

154 La Commission a publié un document intitulé « Deuxième phase de consultation des partenaires sociaux sur la protection des données à caractère personnel des travailleurs », http://europa.eu.int/comm/employment_social/labour_law/docs/secondstageconsultdataprot_fr.pdf.

155 *J.O.C.E.*, n° L 281, 23 novembre 1995, pp. 0031-0050.

156 *J.O.C.E.*, n° L 20, 31 juillet 2002, pp. 0037-0047. Cette directive remplaçait la 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 (*J.O.C.E.*, n° L 024, 30 janvier 1998, pp. 0001-0008).

157 *Cf.* E. Plasschaert et J.-A. Delcorde, « Le traitement des données personnelles des travailleurs », *Orientations*, n° spécial 35 ans, mars 2005, pp. 26 et s.

Dès que des données à caractère personnel sont traitées, qu'il s'agisse d'un enregistrement, d'une communication ou de la simple conservation de données à caractère personnel, le responsable de ce traitement est tenu de se plier aux conditions prévues par la loi. Cette loi impose en particulier le respect d'un principe de transparence, de nécessité et de proportionnalité[158].

80. Elle est applicable tant au contrôle des e-mails qu'à la simple consultation de ceux-ci, comme il ressort notamment de l'avis d'initiative rendu sur cette question par la Commission de la protection de la vie privée[159]. Il importe peu que cet e-mail revête un caractère privé ou professionnel : la loi s'applique dès que l'opération de traitement porte sur des données relatives à une personne physique identifiée ou identifiable[160].

81. L'application de cette loi implique qu'un traitement, comme par exemple la prise de connaissance de courriers électroniques ou de données relatives à l'utilisation d'internet, doit toujours être licite (*cf.* art. 4, § 1er, 1° de la loi du 8 décembre 1992) de sorte que des données à caractère personnel recueillies illicitement, par exemple en violation de l'article 124 de la loi du 13 juin 2005, ne peuvent faire l'objet d'aucun traitement. Par ailleurs, la recommandation nº R (89) 2 du Comité des ministres du Conseil de l'Europe aux États membres sur la protection des données à caractère personnel utilisées à des fins d'emploi, adoptée par le Comité des ministres le 18 janvier 1989, insiste sur la nécessité de dispenser une information préalable aux travailleurs sur les contrôles opérés et préconise même la consultation préalable des travailleurs[161].

---

158 Pour un exposé plus détaillé de cette loi nous vous renvoyons à la contribution de K. Rosier intitulée « Gestion et protection des données dans la relation de travail », au sein du présent ouvrage.

159 Commission de la protection de la vie privée, Avis d'initiative 2000/10 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

160 C. trav. Bruxelles (3e ch.), 8 avril 2003, *Chron. D.S.*, 2005, p. 208 ; C. trav. Bruxelles, 14 décembre 2004, *Computerrecht*, 2005, p. 313 ; Trib. trav. Bruxelles (3e ch.), 13 septembre 2005, R.G. nº 46.114, www.cass.be.

161 Cette recommandation prévoit en son article 3 intitulé « Information et consultation des employés » que :

« 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. »

82. Comme on le verra *infra*, cette loi et l'avis rendu le 3 avril 2000 par la Commission de la protection de la vie privée, relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail[162], ont largement inspiré les principes qui prévalent dans la C.C.T. nº 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau. Ceci dit, le respect de la C.C.T. nº 81 ne suffit pas à satisfaire à toutes les exigences de la loi du 8 décembre 1992 qui reste pleinement applicable.

Section 5
Les conventions collectives de travail

A. La C.C.T. nº 39

83. La C.C.T. nº 39, relative à l'information et à la concertation sur les conséquences sociales de l'introduction de nouvelles technologies, prévoit une obligation d'information et de concertation à charge de l'employeur qui décide d'investir dans une nouvelle technologie, lorsque celle-ci a des conséquences importantes en ce qui concerne l'emploi, l'organisation ou les conditions de travail[163].

Rappelons également le respect de la loi du 20 septembre 1948 portant organisation de l'économie[164] et de la convention collective de travail nº 9 du 9 mars 1972[165]. En vertu de ces textes, le conseil d'entreprise doit être informé et consulté préalablement sur tous projets et mesures susceptibles de modifier la politique du personnel, l'organisation du travail ou les circonstances et les conditions dans lesquelles s'exécute le travail dans l'entreprise ou dans l'une de ses divisions[166].

84. La C.C.T. nº 39 s'adresse aux entreprises qui occupent habituellement au moins 50 travailleurs durant l'année calendrier qui précède. D'autre part, l'employeur ne sera soumis à l'obligation d'information que si cette nouvelle

---

162 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

163 Voy. notamment Th. Claeys, N. Toussaint et D. Dejonghe, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2001, pp. 288-289.

164 *M.B.*, 27-28 septembre 1945.

165 Rendue obligatoire par arrêté royal du 12 septembre 1972 (*M.B.*, 8 février 1984).

166 Voy. notamment Th. Claeys, N. Toussaint et D. Dejonghe, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2001, pp. 288.

technologie a des conséquences collectives importantes en ce qui concerne l'emploi, l'organisation du travail ou les conditions de travail.

L'employeur est tenu, trois mois avant l'introduction de la nouvelle technologie :

– 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
– de procéder à une concertation avec les représentants des travailleurs sur les conséquences sociales de l'introduction de la nouvelle technologie.

85. En vertu de l'article 3 de la C.C.T. nº 39, l'information susvisée doit porter sur la nature de la nouvelle technologie, sur les facteurs économiques, financiers ou techniques qui justifient son introduction, sur la nature des conséquences sociales qu'elle entraîne ainsi que sur les délais de mise en œuvre de la nouvelle technologie.

Dans le cas où l'employeur ne respecte pas le processus d'information et de concertation prévu par la convention collective, tout acte de rupture du contrat de travail par l'employeur donnera lieu à l'indemnisation forfaitaire du travailleur, sauf si cet acte est fondé sur un motif étranger à l'introduction de la nouvelle technologie.

Toutefois, la C.C.T. précise que la charge de la preuve de ces motifs incombera à l'employeur, si la rupture des relations contractuelles intervient dans les trois mois qui suivent le jour où l'information susmentionnée aurait dû être donnée et se terminant trois mois après la mise en œuvre effective de la nouvelle technologie.

86. La C.C.T. ne définit pas ce qu'elle entend par technologie[167]. On peut à titre d'exemple, et en matière informatique, y faire rentrer l'introduction d'un nouveau logiciel de calcul dans l'entreprise. Plus délicate est la question de savoir si la procédure d'information vise également un système de contrôle (de l'utilisation de l'informatique ou du travail) qui serait mis en place par l'employeur. La doctrine est divisée à ce sujet.[168] Selon P. Humblet, le critère

---

167 Le mot « nouvelle » s'entendant par rapport à ce qui se faisait antérieurement dans l'entreprise (commentaire de l'article 2 de la C.C.T. nº 39).

168 Pour une interprétation large du concept, englobant également l'installation de technologies de contrôle : voy. K. Rosier, « Informatique et contrat de travail : introduction de nouvelles technologies dans l'entreprise », *B.S.J.*, nº 355, p. 6 ; semblent également aller dans ce sens : H. Barth, « Emploi, vie privée, et technologies de surveillance », *J.T.T.*, 2002, p. 174 ; G. Demez, « La preuve en droit du travail : protection de la vie privée et nouvelles technologies. Du contremaître à la surveillance », *in Questions de droit social*, Formation permanente série CUP, nº 56, 2002, pp. 315-316. Considèrent que la C.C.T. nº 39 ne s'applique pas à l'introduction de technologies de contrôle : Th. Claeys et D. Dejonghe, « Gebruik van

prédominant pour apprécier si l'introduction d'une nouvelle technologie est sujette à la C.C.T. nº 39, est son impact sur les conditions et l'organisation du travail, à savoir l'accroissement ou la diminution de cet emploi (entraînant, pour reprendre les termes du commentaire de l'article 2 de la C.C.T., un licenciement ou des mutations).

B. La C.C.T. nº 81

1. Présentation de la C.C.T. nº 81

87. Pour répondre au besoin de contrôle des employeurs, et essayer de combler l'absence de réglementation cohérente en la matière, les partenaires sociaux ont négocié la convention collective de travail nº 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau (C.C.T. nº 81)[169].

La C.C.T. nº 81 avait pour objet de clarifier et de préciser les normes fondamentales de manière à assurer leur applicabilité effective dans l'entreprise[170]. Les compromis dégagés ont le mérite de tendre à une pondération des intérêts et droits de chacun et d'instaurer un système de contrôle dont les modalités ont été définies au regard des principes dégagés par la Commission de la protection de la vie privée dans son avis 10/2000 du 3 avril 2000[171].

88. Dans le prolongement des principes issus de la loi du 8 décembre 1992, l'article 4 de la C.C.T. exige le respect des principes de finalité (article 5), de proportionnalité (article 6) et de transparence (article 7). Le premier implique que les contrôles doivent s'inscrire dans les finalités définies dans la C.C.T., le second impose des restrictions en matière d'individualisation des données, tandis que le troisième principe entraîne l'obligation pour l'employeur d'informer les travailleurs au préalable sur les contrôles dont ils peuvent faire l'objet.

La C.C.T. pose le principe selon lequel l'employeur peut déterminer les conditions d'utilisation des outils qu'il met à la disposition de ses travail-

---

e-mail en internet op de werkplaats en contrôle door de werkgever », *J.T.T.*, 2001, p. 132 ; voy. également P. Humblet, « Videocamera 's op de werkplaats : een (zelf)kritiek », note sous Trib. trav. Bruges, 14 mars 1996, *C.D.S.*, 1997, p. 30. Pour plus d'informations sur cette question, voy. également Th. Claeys, N. Toussaint et D. Dejonghe, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau Bruxelles, 2001, pp. 288-289.

169 La C.C.T. nº 81 a été adoptée le 26 avril 2002 et a été rendue obligatoire par arrêté royal du 12 juin 2002, *M.B.*, 26 janvier 2002, p. 29489.

170 Voy. rapport de la C.C.T. nº 81.

171 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

leurs[172]. Elle ne définit toutefois pas quelle est la marge de manœuvre à cet égard puisqu'elle indique dans son préambule que la convention collective de travail ne réglemente pas l'accès et/ou l'utilisation par le travailleur des moyens de communication électroniques en réseau au sein de l'entreprise[173]. Par ailleurs, elle souligne le droit au respect de la vie privée du travailleur sur le lieu du travail. La prise en compte de ce droit conduit la C.C.T. à prévoir expressément que, nonobstant les prérogatives de l'employeur pour régler l'accès et l'utilisation de ces outils de travail, il ne pourra pas effectuer un contrôle de l'utilisation des outils sans respecter certaines conditions définies dans la C.C.T. et qui sont censées garantir ce droit au respect de la vie privée[174].

2. Champ d'application de la C.C.T.

a. Champ d'application personnel

89. En ce qui concerne le champ d'application personnel, il n'est pas inutile de rappeler que la C.C.T. nº 81 ne lie que les employeurs du secteur privé et n'est donc pas applicable dans le secteur public[175].

b. Champ d'application matériel

90. Le champ d'application matériel est spécifié à l'article 1, § 1er de la C.C.T. qui définit à quelles conditions de proportionnalité et de transparence un contrôle des données de communication électroniques en réseau peut être installé et les modalités dans lesquelles l'individualisation de ces données est autorisée.

1. Contrôle des données relatives aux communications électroniques transitant par réseau

91. Les dispositions de la C.C.T. ne réglementent que les contrôles effectués sur des données de communication électroniques en réseau, à savoir les données « relatives aux communications électroniques transitant par réseau, entendues au sens large et indépendamment du support par lequel elles sont transmises ou reçues par un travailleur dans le cadre de la relation de travail »[176]. Ce terme renvoie aux notions de réseau de communications électroniques et de services

172 Art. 1 § 2 et article 3 de la C.C.T nº 81.

173 C.C.T. nº 81, art. 1, § 2.

174 O. Rijckaert, « La protection de la vie privée du travailleur : principes et cadre juridique », *in Surveillance électronique des travailleurs et usage des TIC à des fins privées sur le lieu de travail*, FEB, Bruxelles, 2002, p. 41.

175 Nous vous renvoyons à cet égard à la contribution de D. De Roy publié dans le cadre du présent ouvrage et qui traite des spécificités du secteur public à cet égard.

176 C.C.T. nº 81, art. 2.

de communications électroniques, dont on trouve la définition à l'article 1er de la loi du 13 juin 2005 relative aux communications électroniques qui remplace la loi du 21 mars 1991 à laquelle la C.C.T. fait d'ailleurs explicitement référence[177]. Comme mentionné ci-avant[178], par « données de communication électroniques », on vise les données relatives aux communications électroniques qui transitent par réseau telles l'adresse e-mail de l'expéditeur et du destinataire, l'heure de l'envoi et de la réception, les données de routage, la taille du message, la présence de pièces jointes, les données de connexion à internet etc.[179].

92. Aux termes du commentaire de l'article 1er de la C.C.T., il est précisé que « La présente convention collective de travail entend ici définir un cadre suffisamment large pour englober l'ensemble des technologies en réseau tout en ne perdant pas de vue l'imbrication croissante et l'évolution rapide de ces technologies et du support auquel elles recourent. Elle s'applique en conséquence indépendamment de ce support. Elle vise par ailleurs les communications électroniques en réseau tant interne qu'externe ».

Ainsi les contrôles visés sont-ils potentiellement très larges et concernent-ils à la fois les communications sur un réseau interne à l'entreprise (tel un intranet) que sur un réseau externe (tel l'internet).

En ce sens, la Cour du travail d'Anvers a considéré que ce qui importe n'est pas la technologie utilisée mais le fait que le contrôle porte sur des communications réalisées dans le cadre ou, du moins, pendant la durée du travail[180]. Dans le même sens, le Tribunal du travail de Liège a estimé que le fait que les e-mails litigieux avaient été adressés à partir d'une boîte mail privée Yahoo (et non via la boîte e-mail professionnelle de l'entreprise) ne faisait pas obstacle à l'application de la C.C.T. dès lors que ceux-ci avaient été envoyés grâce à l'utilisation du matériel de l'entreprise[181].

93. Compte tenu du libellé extrêmement large du champ d'application de la C.C.T, on peut se demander si celle-ci a ou non vocation à s'appliquer aux contrôles effectués sur toutes les données transitant par réseau (telles les données de communication téléphone fixe ou mobile, ou encore les données de géolocalisation). Il existe, en effet, une multitude de données qui transitent

---

177 La C.C.T. renvoyait à la terminologie de l'ancienne loi du 21 mars 1991, qui visait alors les « télécommunications », terme remplacé par celui de « communications électroniques ».

178 Chapitre 2, section 3, A.

179 O. Rijckaert, « Le contrat de travail face aux nouvelles technologies », *Orientations*, 2000, p. 210. Pour un cas d'application voyez : C. trav. Anvers, 10 février 2004, disponible sur www.cass.be.

180 C. trav. Anvers (sect. Hasselt), 2 septembre 2008, R.G. nº 2070230, *DAOR*, 2010, liv. 95, p. 336, note van Bever ; *Orientations*, 2008 (reflet I. Plets), liv. 9, p. 261 ; pour un commentaire de cette décision voy. : K. Rosier, « Le cybercontrôle des travailleurs contrôlé par le Juge », *Orientations*, 2009, nº 413, p. 22.

181 Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. nº 360.454, www.cass.be.

par un réseau de communication électronique au sens de la loi du 13 juin 2005, laquelle n'entend pas uniquement régir les services de communications électroniques que sont les connexions à internet et les e-mails. Les communications satellitaires et téléphoniques sont expressément incluses dans le champ d'application de la loi.

En faveur d'une interprétation large du champ d'application de la C.C.T., on relèvera que l'article 2 de la C.C.T. précise que « Pour l'application de la présente convention collective de travail, on entend par données de communication électroniques en réseau les données relatives aux communications électroniques transitant par réseau, entendues au sens large et indépendamment du support par lequel elles sont transmises ou reçues par un travailleur dans le cadre de la relation de travail ». Dans le commentaire de cette disposition, la volonté de donner un champ d'application technologiquement neutre est confirmée et il y est rappelé que la convention collective de travail entend définir un cadre suffisamment large pour englober l'ensemble des technologies en réseau tout en ne perdant pas de vue l'imbrication croissante et l'évolution rapide de ces technologies et du support auquel elles recourent. En ce sens également, on relèvera l'objectif que se donne la convention et qui est, selon les termes du préambule de celle-ci, « de veiller à garantir le respect de la vie privée du travailleur lorsqu'une collecte de données de communications électroniques en réseau est instaurée sur le lieu de travail pour en faire le contrôle et dans ce cadre, les traiter de manière à les attribuer à un travailleur ».

94. Il nous semble donc que le champ d'application de la C.C.T. peut potentiellement inclure d'autres technologies que l'e-mail ou l'internet[182] et que pourraient dès lors être concernées les collectes d'informations relatives à toute donnée transitant par réseaux de communication électronique utilisé au sein de l'entreprise, ces réseaux lui appartenant ou non (réseau de téléphonie mobile, réseau satellite pour localisation GPS, réseau wifi de l'entreprise…)[183]. On relèvera toutefois que ces autres modes de communications ne sont pas évoqués dans la C.C.T. alors que l'usage du téléphone et même du GSM étaient déjà présents lors de son adoption. Il n'y a pas d'allusion à ces communications alors qu'il est expressément question d'e-mails, de l'usage d'internet, de système informatique. En outre, il convient de garder à l'esprit que la C.C.T. s'est donnée pour vocation de préciser comment appliquer les dispositions légales (essentiellement celles de la loi du 8 décembre 1992) dans le contexte spécifique de contrôles de données dans la relation de travail.

---

182 Voy. en ce sens, T. Messiaen, « Navigatiesysteem en privacy », *NjW*, nº 161, 2007, p. 339.

183 Voy. en ce sens, P. Degouis et S. van Wassenhove, *Nouvelles technologies et leur impact sur le droit du travail*, Courtrai, UGA, 2010, p. 72.

C'est ainsi qu'elle dégage des finalités légitimes eu égard au contexte et aux intérêts des parties en présence. On peut se demander si les principes dégagés spécifiquement, semble-t-il, pour le contrôle de l'usage de l'e-mail et d'internet peuvent s'appliquer tels quels pour la géolocalisation, par exemple. On verra que les seules finalités de contrôle admises dans le cadre de la C.C.T. ne sont pas vraiment pertinentes au regard des objectifs que peut poursuivre un contrôle par le biais de la géolocalisation ou le contrôle des factures de téléphone d'un travailleur.

Toujours est-il que la jurisprudence actuelle ne s'est à notre connaissance pas prononcée sur l'application de la C.C.T. à d'autres contrôles de communication que ceux effectués sur des e-mails ou sur l'usage d'internet.

2. Exclusion du contenu des communications électroniques

95. Conformément à la précision apportée dans le rapport préalable de la C.C.T., le contenu des données de communication électroniques est exclu du champ d'application de la C.C.T. [184]. Ceci rejoint la position de la Commission de la protection de la vie privée qui avait considéré que, « en ce qui concerne le courrier électronique, […] 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. […] 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 » [185].

Cette exclusion implique qu'en toute hypothèse seuls des contrôles ayant pour résultat de mettre en évidence des données relatives aux communications (adresses des expéditeurs et destinataires, dates des communications, date et heures de connexion à l'internet, URL des sites visités, etc.) sont visés par la C.C.T. et que l'employeur ne pourra prendre connaissance du contenu des e-mails concernés ni des pages visitées.

---

184 O. Rijckaert, « La protection de la vie privée du travailleur : principes et cadre juridique », *in Surveillance électronique et travailleurs et usage des TIC à des fins privées sur le lieu de travail*, FEB, 2002, p. 41. La frontière entre données de communication et contenu nous semble difficile à tracer dès lors que, par exemple, une adresse IP constitue plutôt une donnée de communication mais révèle clairement le contenu consulté (voy. à cet égard n° 20 et 21, *supra*).

185 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

3. Exclusion des e-mails dont le caractère professionnel n'est pas contesté par le travailleur

96. L'article 11, al. 3 de la C.C.T. nº 81 mentionne que « lorsque l'objet et le contenu des données de communication électroniques en réseau ont un caractère professionnel non contesté par le travailleur, l'employeur pourra les consulter sans autre procédure ».

Il en résulte clairement que les partenaires sociaux ont entendu exclure de la procédure de contrôle imposée par la C.C.T. les communications dont la nature professionnelle n'est pas contestée par le travailleur[186]. La C.C.T. reste toutefois muette sur la définition des communications de nature professionnelle.

En application de ce principe, plusieurs décisions du Tribunal du travail de Liège distinguent e-mails professionnels et courriers privés en précisant que les e-mails adressés via une adresse de messagerie professionnelle ont *a priori* un caractère professionnel. Elles n'examinent la régularité du contrôle qu'après avoir constaté le caractère « mixte » (privé/professionnel) des e-mails concernés[187].

Nous reviendrons sur cette distinction de régimes qui nous semble critiquable au regard de la loi[188].

3. Modalités de contrôle

97. La C.C.T. établit une série de principes qui précisent ceux déjà exposés ci-dessus et consacrés par les articles 8, de la C.E.D.H., 22 de la Constitution et par la loi du 8 décembre 1992.

a. Les finalités légitimes

98. La C.C.T. mentionne, en son article 5, quatre finalités considérées comme légitimes. Selon la C.C.T., seules ces finalités qu'elle édicte sont susceptibles de légitimer le contrôle de données de communication électroniques par l'employeur. Cette liste est donc exhaustive et tout contrôle rentrant dans le champ d'application de la C.C.T. ne pourra avoir d'autre but que ceux édictés par

---

186 O. Rijckaert, « La protection de la vie privée du travailleur : principes et cadre juridique », *in Surveillance électronique et travailleurs et usage des TIC à des fins privées sur le lieu de travail*, FEB, 2002, p. 41. Sur la légalité de l'article 11 de la C.C.T., voy. toutefois le point 4, *infra*.

187 Trib. trav. Liège (3e ch.), 3 septembre 2008, R.G. nº 371.015, www.cass.be ; Trib. trav. Liège (3e ch.), 19 mars 2008, R.G. nº 360.454, www.cass.be. Voyez également la décision du Tribunal du travail de Gand du 1er septembre 2008 au sein de laquelle le tribunal suggère que lorsque le contrôle porte sur des e-mails professionnels, il appartiendrait au travailleur de prouver en quoi son droit au respect de la vie privée serait violé (Trib. trav. Gand, 1er septembre 2008, R.G. nº 17054/06, www.cass.be).

188 Voy. point 4 *infra*, nº 105 et suiv.

l'article 5. Il est à noter toutefois qu'elle précise dans le même temps que les modalités définies dans la C.C.T. ne s'appliquent que lorsque le contrôle s'inscrit dans ces finalités doublées d'un objectif de surveillance. La C.C.T. laisse, selon ses propres termes, en l'état la possibilité d'utiliser des contrôles de données de communication électroniques en réseau à des fins de formation étant donné qu'il ne s'agit pas de surveillance[189]. On peut à cet égard regretter que la C.C.T. ne donne pas de définition des termes « contrôle » et « surveillance », au centre de ce texte. Ainsi, on peut se demander si le traitement de données de communication à des fins d'évaluation de la productivité doit être considéré ou non comme une surveillance au sens de la C.C.T.[190]

Ceci étant dit, les finalités dont question sont[191] :

1° la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;

2° 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 ;

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

4° le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

Nous verrons que la C.C.T. n'autorise l'individualisation directe des données de communication électroniques que si la finalité poursuivie est l'une des trois premières citées. Dans le cas d'un contrôle effectué pour vérifier le respect des règles d'utilisation des outils de communication électronique, la C.C.T. prévoit une procédure spécifique.

b. L'obligation d'information

§ 1er. Le contenu de l'information

99. La C.C.T. nº 81 prévoit également une obligation d'information, laquelle est soit collective, soit individuelle en fonction des informations concernées.

189 C.C.T. nº 81, commentaire de l'article 5.

190 Dans la négative, il est à noter que le contrôle de ces données pourrait tout de même constituer une finalité légitime au sens de la loi du 8 décembre 1992 même si elle n'est pas mentionnée par l'article 5 de la convention collective.

191 Nous renvoyons aux commentaires de l'article 5 de la C.C.T. pour de plus amples développements à cet égard.

L'information collective et individuelle porte sur les aspects suivants du contrôle des données de communication électroniques en réseau :

- la politique de contrôle ainsi que 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, ainsi que le lieu et la durée de conservation ;
- 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 ;
- les droits, devoirs, obligations des travailleurs et les interdictions éventuelles prévues dans l'utilisation des moyens de communication électronique en réseau de l'entreprise ;
- les sanctions prévues au règlement de travail en cas de manquement[192].

§ 2. Modalités de l'information

100. En ce qui concerne l'information collective, l'employeur qui souhaite installer un système de contrôle des données de communication électroniques en réseau, informe le conseil d'entreprise sur tous les aspects du contrôle visés à l'article 9, § 1er de la C.C.T., conformément aux dispositions de la convention collective de travail nº 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise[193]. À défaut de conseil d'entreprise, cette information est fournie au comité de la prévention et de la protection du travail ou, à défaut, à la délégation syndicale ou, à défaut, aux travailleurs.

En ce qui concerne l'information individuelle, le support de l'information individuelle est laissé à l'appréciation de l'employeur[194].

À cet égard, précisons toutefois que l'article 6, 5° de la loi sur les règlements de travail impose que ce dernier stipule les droits et obligations du personnel de surveillance. On peut donc en conclure que si l'employeur veut

---

192 Art. 8 de la C.C.T.

193 Art. 7 de la C.C.T.

194 Selon la C.C.T. nº 81, elle pourra être réalisée :
- dans le cadre d'instructions générales (circulaires, affichage, etc.) ;
- par mention dans le règlement de travail ;
- par mention dans le contrat de travail individuel ;
- 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).

confier à son personnel des missions de surveillance, il doit encadrer les pouvoirs de ce personnel dans le règlement de travail adapté à cet effet[195].

En outre, l'article 8 de la C.C.T. renvoie au règlement de travail pour préciser les sanctions qui résultent du non-respect de la politique d'utilisation des moyens informatiques.

Par conséquent, une modification du règlement de travail sera en principe nécessaire dans le cas où l'employeur désire implémenter une politique de contrôle de l'utilisation des moyens de communication électronique[196].

101. La C.C.T. n'impose aucune obligation de concertation. Toutefois, rappelons que la C.C.T. nº 39 examinée ci-dessus préconisait une telle concertation en cas d'introduction de nouvelles technologies dans l'entreprise, ce qui arrivera parfois simultanément avec la mise en place d'une politique de contrôle[197].

102. Soulignons également qu'en vertu de l'article 10 de la C.C.T. nº 81, il est prévu que les systèmes de contrôle fassent régulièrement l'objet d'une évaluation selon le cas, au sein du conseil d'entreprise, du comité pour la prévention et la protection au travail ou avec la délégation syndicale, et ce, précise cette disposition, « de manière à faire des propositions en vue de les revoir en fonction des développements technologiques ».

c. Le mécanisme de contrôle instauré par la C.C.T. nº 81

§ 1er. Respect du principe de proportionnalité

103. L'article 6 de la C.C.T. consacre le principe de proportionnalité et dispose que, « par principe, le contrôle des données de communication électroniques en réseau ne peut entraîner une ingérence dans la vie privée du travailleur. Si toutefois ce contrôle entraîne une ingérence dans la vie privée du travailleur, cette ingérence doit être réduite à un minimum. »

Le commentaire de cet article précise que, selon ce principe, l'employeur ne pourra collecter en vue du contrôle que les données nécessaires à la finalité poursuivie, c'est-à-dire les données qui entraînent l'ingérence la plus réduite

---

195 S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2005, p. 163.

196 Rappelons en effet que l'information doit porter à la fois sur les règles d'utilisation et sur le contrôle du respect de celles-ci. Les sanctions éventuelles en cas de non-respect de ces règles devront quand à elles figurer au règlement de travail.

197 Voy. O. RIJCKAERT, « Le contrôle de l'usage de l'internet et de l'*e-mail* sur le lieu de travail, au regard de la convention collective de travail nº 81 du 26 avril 2002 », *Guide Social Permanent*, Kluwer, juin 2002, nº 135, p. 17.

dans la sphère privée du travailleur. Le contrôle doit en effet revêtir un caractère adéquat, pertinent et non excessif au regard des finalités poursuivies[198].

À titre d'exemple, le contrôle des sites internet et des e-mails devra donc idéalement passer par un examen global du listing des sites visités et du nombre d'e-mails envoyés et de leurs caractéristiques (taille, pièces jointes, fréquence,..), mais ne devra pas faire l'objet d'une individualisation systématique aboutissant à l'identification des travailleurs[199].

C'est d'ailleurs pour préserver ce principe de proportionnalité que la C.C.T. prévoit un mécanisme d'individualisation particulier dont l'application diffère en fonction de la finalité poursuivie. Nous examinons ci-dessous la procédure d'individualisation imposée par la C.C.T.

§ 2. Procédure d'individualisation

104. En ce qui concerne les modalités du contrôle, la C.C.T. distingue deux hypothèses. Dans la première, l'employeur est autorisé à procéder à l'individualisation directe des données de communication électroniques. Dans la seconde hypothèse, l'employeur devra respecter une procédure d'avertissement préalable avant d'individualiser lesdites données.

Lorsque la finalité du contrôle est l'une des trois premières finalités visées à l'article 5, § 1 de la C.C.T., l'employeur est autorisé, à partir des données globales dont il dispose, à procéder à une individualisation des données de manière à retracer l'identité de la personne responsable de l'anomalie qu'il a constatée[200].

Cela signifie qu'une fois une anomalie constatée sur la base de données non individualisées, l'employeur est autorisé à procéder à l'identification de l'utilisateur du moyen de communication électronique ayant donné lieu à l'anomalie. Une fois cette individualisation constatée, l'employeur pourra prendre la décision qu'il estime adéquate : soit une sanction disciplinaire[201], soit une audition du travailleur, soit son licenciement pour motif grave[202].

---

198 Art. 14 de la C.C.T ; B. Geradin, « La Convention collective de travail relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électronique en réseau du 26 avril 2002, p. 16, disponible sur www.droit-technologie.org.

199 Voy. commentaire de l'article 6 de la C.C.T et S. van Wassenhove, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2005, p. 171.

200 Art. 15 de la C.C.T.

201 Pour autant que cette possibilité soit prévue dans le règlement de travail.

202 S. van Wassenhove, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2005, p. 172.

La Cour du travail de Liège a ainsi considéré que « dès lors que l'employeur a connaissance, de quelque manière que ce soit, d'une possible attaque de son système par un virus, un ver, un cheval de Troie ou autre, ou d'une menace d'une telle attaque, il se trouve incontestablement dans une situation visée à l'article 4, 3° précité qui l'autorise à procéder à un contrôle des données de communication »[203]. La Cour a également estimé que, « en l'espèce, en découvrant un échange de messages entre deux travailleurs ayant accès à son système qui évoque la possibilité d'introduire un virus dans ledit système, la SA est fondée à procéder à un contrôle des données échangées entre ces travailleurs ».

La Cour a donc fait application du principe de finalité, jugeant que le contrôle portait bien sur la sécurité du système informatique, et permettait donc une individualisation directe. La Cour a également considéré que le principe de transparence avait été respecté dès lors qu'aucun système de contrôle particulier n'avait été installé, l'accès à la messagerie interne étant apparemment ouvert à tous, sans code d'accès.

105. Toutefois, la C.C.T. prévoit une procédure spécifique lorsque la finalité poursuivie par l'employeur à l'occasion du contrôle est la dernière finalité prévue par l'article 5, § 1 de la C.C.T., à savoir le contrôle du respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

Dans ce cas, l'employeur devra, avant de procéder à une individualisation, porter à la connaissance des travailleurs, de manière certaine et compréhensible, l'existence de l'anomalie et les avertir qu'il sera procédé à une individualisation des données de communication électroniques en réseau si une nouvelle anomalie de même nature est constatée.

L'information donnée au travailleur précisera la nature de l'anomalie constatée et indiquera qu'en cas de nouvelle anomalie, aucune nouvelle mise en garde ne sera communiquée avant l'individualisation, le cas échéant.

L'article 17 de la C.C.T. ajoute que le travailleur auquel une anomalie d'utilisation des moyens de communication électronique en réseau peut être attribuée par application et à l'issue de la procédure d'individualisation indirecte visée à l'article 16, sera invité à un entretien par l'employeur. Cet entretien devra précéder toute décision ou évaluation susceptible d'affecter individuellement le travailleur.

L'objectif de cette disposition est de permettre au travailleur de faire valoir ses objections et justifications éventuelles et de s'expliquer sur l'utili-

[203] C. trav. Liège, 20 mars 2006, R.G. nº 33137-05, www.cass.be.

sation faite des moyens de communication électronique en réseau mis à sa disposition.

Toutefois, on peut se demander, comment, en pratique, cette procédure d'individualisation sera suivie dès lors que, bien souvent, l'employeur aura déjà pu examiner les données de trafic (voire leur contenu) et identifié leur auteur avant d'avoir averti les travailleurs[204]. Les principes de la C.C.T. risquent donc de rester un vœu pieux des partenaires sociaux.

Un arrêt rendu par la Cour du travail d'Anvers illustre d'ailleurs le fait qu'il est parfois difficile de distinguer en pratique les finalités de contrôle[205]. En l'espèce, le contrôle avait été effectué par un responsable IT qui avait commencé par repérer une utilisation suspecte des ressources informatiques de l'entreprise de par l'utilisation d'une connexion et d'un *firewall* nouvellement installé dans le chef de plusieurs travailleurs avant, dans un second temps, de constater que le trafic internet était particulièrement élevé pour un seul de ces travailleurs. S'il s'agissait au départ de vérifier le bon fonctionnement du réseau, la poursuite du contrôle visait à contrôler le respect du règlement IT de l'entreprise - qui ne permettait qu'un usage exceptionnel d'internet à des fins privées en dehors des périodes de pause. Le travailleur mettait en cause la régularité du contrôle notamment eu égard au fait qu'il avait été immédiatement procédé à une individualisation des données sans phase d'information préalable, ce qui n'était pas contesté. La Cour estimera notamment que dès lors que le contrôle poursuivait au moins pour une part une finalité de protection de la sécurité et du bon fonctionnement du système informatique de l'entreprise, il n'était pas nécessaire que l'employeur passe par une phase d'alerte avant d'individualiser les données. Cette conclusion semble toutefois critiquable eu égard à l'article 14 de la C.C.T. dont il résulte que la possibilité d'individualiser des données est indissociable de la finalité du contrôle dans laquelle elle s'inscrit[206].

4. Appréciation critique de la C.C.T. nº 81

106. Le contrôle des moyens de communication électronique (conversations téléphoniques, e-mails et internet, par exemple) s'inscrit dans le cadre législatif plus large - décrit ci-dessus[207] - que celui de la C.C.T. nº 81 et qui proscrit,

---

204 En ce sens: O. RIJCKAERT, « Surveillance des travailleurs: nouveaux procédés, multiples contraintes », *Orientations*, nº spécial 35 ans, mars 2005, pp. 52-53.

205 C. trav. Anvers (section Hasselt), 2 septembre 2008, *DAOR*, 2010, liv. 95, p. 336, note VAN BEVER; *Orientations*, 2008 (reflet I. Plets), liv. 9, p. 261.

206 K. ROSIER, « Le cybercontrôle des travailleurs contrôlé par le Juge », *Orientations*, 2009, p. 25.

207 Outre l'application des articles 8 de la C.E.D.H. et 22 de la Constitution, il y lieu de tenir compte de l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques (anciennement, article 109*ter* D de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques) et de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements

en principe, la prise de connaissance des données de communication électroniques sans le consentement de toutes les parties concernées. Ce consentement est la plupart du temps impossible à obtenir du fait notamment que des tiers à l'entreprise sont généralement concernés. Cette réglementation est donc très rigide puisqu'elle n'opère aucune distinction entre le sort à réserver aux communications électroniques de nature professionnelle et celles à caractère privé.

107. Si la C.C.T. offre un cadre très utile pour permettre un certain contrôle de l'employeur quant à l'utilisation par les employés des moyens de communication électronique, on peut toutefois s'interroger sur la validité des dérogations aux dispositions constitutionnelles et légales précitées, que la C.C.T. contient[208]. En particulier, il nous semble douteux, sur le plan légal, que la C.C.T. s'affranchisse de toute règle en matière de contrôle des communications électroniques dont le caractère professionnel n'est pas contesté par le travailleur dès lors que la loi n'opère aucune distinction entre courriers privés et professionnels. Un arrêt de la Cour du travail d'Anvers du 15 décembre 2004 en fait d'ailleurs le constat et indique que la C.C.T. ne confère pas à l'employeur un droit illimité et inconditionnel de prendre connaissance de l'existence et du contenu de communications à caractère professionnel entre un travailleur et un tiers[209]. Celle-ci a considéré que l'affirmation contenue dans le préambule de la C.C.T. n° 81 aux termes de laquelle « lorsque l'objet et le contenu des données de communication électroniques en réseau ont un caractère professionnel non contesté par le travailleur, l'employeur pourra les consulter sans autre procédure » et reprise à l'article 11, al. 3 de la convention est contraire à l'article 8 de la C.E.D.H. ainsi qu'aux articles 314*bis* du Code pénal et à l'article 109*ter* D de la loi du 21 mars 1991 et à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel[210]. L'exclusion des e-mails dont le caractère professionnel n'est pas contesté du champ d'application de la C.C.T. est donc remis en cause par la Cour qui considère que cette distinction n'est pas justifiée.

---

de données à caractère personnel qui s'applique dès lors que la prise de connaissance d'un courrier électronique, qu'il s'agisse de données de communication ou du contenu, implique le traitement de données relatif à une personne physique.

208 Avec O. Rijckaert, nous considérons qu'une convention collective de travail, fût-elle rendue obligatoire par arrêté royal, ne peut déroger à une disposition contenue dans une loi et dont le non-respect est, du reste, sanctionné pénalement (O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 43 ; voy. également en ce sens, J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, pp. 33 et s.).

209 C. trav. Anvers (section. Anvers), 15 décembre 2004, R.G. n° 2004-0295, www.cass.be.

210 C. trav. Anvers (section. Anvers), 15 décembre 2004, R.G. n° 2004-0295, www.cass.be.

108. Les possibilités de contestation de la validité de la C.C.T. sont donc nombreuses et ne font qu'ajouter de l'insécurité juridique là où la complexité existait déjà. Nous rappelerons encore que la question de la violation de l'article 22 de la Constitution est également posée dès lors que la C.C.T. n'a pas valeur de loi et ne peut dès lors réglementer des matières touchant à la protection de la vie privée des individus[211].

109. Ceci étant, on constatera que la jurisprudence s'est majoritairement employée à prendre en compte cette C.C.T. sans en questionner la légalité ou sa constitutionnalité[212].

Ainsi, dans un arrêt du 13 septembre 2005, la Cour du travail de Bruxelles a déjà pu considérer que la C.C.T. nº 81 ne faisait que clarifier les principes constitutionnels et légaux afin d'être appliqués à la relation entre employeurs et employés[213]. À ce titre, la Cour a considéré que l'employeur ne démontrait pas avoir informé le travailleur de l'existence et des modalités du contrôle effectué, par application de la C.C.T. nº 81, violant ainsi le principe de général de transparence que cette convention consacre. La Cour ajoute que, dès l'instant où l'employeur confirmait que les communications collectées n'étaient pas de nature professionnelle, il pouvait encore plus difficilement soutenir qu'il pouvait prendre connaissance des e-mails sans respecter la procédure prévue par la C.C.T. nº 81.

Chapitre 3
L'établissement d'un règlement d'utilisation et la mise en œuvre du controle

Section 1
Introduction

110. Face à un cadre juridique complexe, voire déroutant, le besoin de réglementer l'utilisation des technologies au sein de l'entreprise se fait vite ressentir ne serait-ce que pour désamorcer les risques de conflit en assurant une transparence de la politique de l'entreprise en termes d'utilisation du matériel et de possibles contrôles.

---

211 *Cf.* chapitre 2, section 2 B,2, *supra*.

212 Voy. notamment : C. trav. Anvers (section Hasselt), 2 septembre 2008, *DAOR*, 2010, liv. 95, p. 336 ; *Orientations*, 2008 (reflet I. Plets), liv. 9, p. 261 ; Trib. trav. Liège (3e ch.), 3 septembre 2008, R.G. nº 371.015, www.cass.be ; C. trav. Anvers (section Hasselt), 15 novembre 2005, *Chron. D.S.*, 2006, p. 153 ; C. trav. Liège (section Namur), 11 janvier 2007, *R.R.D.*, 2007, p. 488, note K. Rosier et S. Gilson ; C. trav. Bruxelles, 13 septembre 2005, *Computerrecht*, 2006, p. 100.

213 C. trav. Bruxelles, 13 septembre 2005, R.G. nº 46114, www.cass.be.

111. Par ailleurs, l'établissement d'un règlement d'utilisation des nouvelles technologies mises à disposition des travailleurs constitue une étape préalable à certains contrôles que l'employeur voudrait effectuer sur les activités de ses travailleurs. Ainsi, loin d'être une pure faculté laissée à l'employeur, l'élaboration d'une telle réglementation sera même nécessaire pour rencontrer les prescriptions légales en matière d'information des travailleurs, que celles-ci résultent des textes réglementant la protection de la vie privée ou les relations de travail.

Cette obligation d'information des membres du personnel fera le plus souvent l'objet d'un document reprenant l'ensemble des dispositions relatives à l'usage des outils informatiques, incluant les règles d'utilisation et les modalités du contrôle du respect de celles-ci.

Ce document, parfois appelé « Charte informatique », « Code de bonne conduite », « *IT Policy* » ou encore « Règlement d'utilisation », contiendra un arsenal plus ou moins important de dispositions, allant des interdictions et autorisations d'utilisation aux différentes sanctions, en passant par les modalités de contrôle.

Section 2
La réglementation de l'usage du matériel informatique et des moyens de communications électroniques

112. Plusieurs questions se posent autour de l'élaboration d'un document réglementant l'utilisation des technologies.

113. La première est de déterminer quelle est la marge de manœuvre de l'employeur en ce qui concerne la réglementation de l'usage des outils de communication mis à la disposition des travailleurs. Cette réflexion ne doit pas forcément être cantonnée à l'usage de l'internet et de l'e-mail mais peut aussi inclure des réflexions sur le stockage d'informations personnelles sur le disque dur des ordinateurs de l'entreprise ou sur des serveurs, ou sur les précautions à prendre concernant l'usage de ces ordinateurs (confidentialité de mots de passe, connexion de matériel étranger à l'entreprise, installation / téléchargement de logiciels sur les PC de l'entreprise, etc.) (*cf.* section A, *infra*).

114. La seconde question a trait à la manière dont la réglementation devra concrètement être réalisée. En premier lieu, nous examinerons le contenu-même de la charte informatique : quels sont les éléments qui doivent y figurer, ceux qui sont optionnels mais recommandés, les limites et possibilités qu'offre la rédaction d'un tel texte (*cf.* section B, *infra*). En second lieu, nous verrons quel support utiliser pour diffuser la politique d'usage des technologies au sein

de l'entreprise (papier, format électronique, règlement de travail ou annexe au contrat de travail,..) (*cf.* section C, *infra*).

A. Quelle marge de manœuvre pour l'employeur ?

115. Comme nous l'avons souligné ci-avant[214], l'employeur peut décider de l'utilisation qui sera ou non permise des moyens de communications électroniques ou plus généralement du matériel mis à disposition des travailleurs. Outre les utilisations qui en seront autorisées, interdites ou tolérées, il appartient à l'employeur de déterminer de quels moyens les travailleurs pourront disposer pour travailler.[215]

Il est clair que l'implémentation de solutions techniques et organisationnelles sont autant d'options que l'employeur pourra mettre en place : disposer les écrans à la vue de tous, bloquer l'accès à certains sites web, limiter la taille des fichiers pouvant transiter par courrier électronique, ou encore ne pas donner l'accès à internet à certaines personnes. On veillera toutefois à ne pas discriminer les travailleurs face à ces décisions.[216]

116. La mise en place de mesures techniques et/ou organisationnelles est sans doute la meilleure manière de respecter la vie privée des travailleurs, dès lors qu'elles sont peu intrusives et relèvent plutôt de l'implémentation de la politique de l'entreprise que de la surveillance et du contrôle. D'ailleurs, à cet égard, le Groupe de l'Article 29[217] préconise que, « dans la mesure du possible, la prévention devrait l'emporter sur la détection. En d'autres termes, il est davantage dans l'intérêt de l'employeur de prévenir l'utilisation abusive de l'internet par des moyens techniques plutôt que de consacrer des ressources à sa détection. Dans la limite de ce qui est raisonnablement possible, la politique de l'entreprise concernant l'internet devrait s'appuyer sur des outils techniques visant à limiter l'accès plutôt que sur des dispositifs de contrôle des comportements, par exemple par des systèmes verrouillant l'accès à certains sites ou générant des avertissements automatiques ».[218] Des systèmes interdisant l'accès

---

214 *Cf.* chapitre 2, section 2, A.

215 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid, Gent, Story*, 2008, p. 38.

216 Ainsi, on peut difficilement imaginer que seuls certains travailleurs ne puissent pas envoyer d'e-mails privés alors que les autres y sont autorisés sans justification objective.

217 Ce groupe, qui tient son nom du fait qu'il a été institué par l'article 29 de la directive 95/46/CE, est un organe consultatif européen, composé en autres de représentants de chaque autorité de contrôle des États membres et qui rend des avis sur l'application de la législation sur la protection des données à caractère personnel.

218 Groupe de l'Article 29, Document de travail concernant la surveillance des communications électroniques sur le lieu de travail, WP55, 29 mai 2002, http://ec.europa.eu/justice, p. 25.

à certains sites prédéterminés par l'employeur, tels Facebook par exemple, sont donc licites.

117. Une question qui se pose toutefois est de savoir si l'employeur peut interdire totalement l'utilisation privée des moyens de communications qu'il met à disposition des travailleurs.

L'arrêt *Niemietz*[219] de la Cour européenne des droits de l'homme, déjà cité, confirme que les personnes développent une partie importante de leurs relations avec le monde extérieur et leur droit à la liberté d'expression joue donc assurément un rôle dans ce contexte. Faut-il en déduire une obligation de mettre à disposition de tels outils ? Nous ne le pensons pas. Il nous semble que si l'on admet que c'est l'employeur qui détermine quels sont les outils de travail mis à la disposition de ses préposés et quelles en seront les modalités d'utilisation, il devrait pouvoir interdire tout usage à des fins privées.

Dès lors, il s'agit là, selon nous, essentiellement d'une question d'opportunité vis-à-vis du personnel. C'est en ce sens que la Commission belge de la protection de la vie privée considère que « le lieu de travail étant le lieu le plus propice pour entretenir des contacts avec des collègues et même avec des personnes extérieures, les employeurs doivent faire preuve d'une certaine tolérance quant aux communications privées passées par les membres de leur personnel à l'aide de leurs moyens de communication ».[220] Son pendant français, la Commission nationale Informatique et Liberté, constate quant à elle qu'« une interdiction générale et absolue de toute utilisation d'internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de l'information et de la communication, et semble de plus disproportionnée au regard des textes applicables et de leur interprétation par la jurisprudence. Un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau ne mettant pas en cause la productivité est généralement et socialement admis par la plupart des entreprises ou administrations. Aucune disposition légale n'interdit évidemment à l'employeur d'en fixer les conditions et limites, lesquelles ne constituent pas, en soi, des atteintes à la vie privée des salariés ou agents publics »[221].

118. Quoi qu'il en soit, ce n'est pas parce que l'employeur interdit toute utilisation non professionnelle des outils de communication électronique qu'il sera

---

219 C.E.D.H., *Niemietz c. Allemagne*, 16 déc. 1992, *Publ. Cour. eur. D.H.*, série A, n° 251-B.

220 Commission de la protection de la vie privée, Avis n° 21 relatif au code de déontologie concernant l'utilisation des moyens informatiques et le traitement électronique de données au sein du Service public fédéral Économie, PME, Classes moyennes et Énergie, 12 juillet 2006, www.privacycommission.be, p. 5.

221 CNIL, *Guide pratique pour les employeurs*, octobre 2005, p. 11, disponible sur www.cnil.fr.

autorisé à contrôler les communications de ses travailleurs sans respecter les principes exposés ci-avant.

B. Éléments susceptibles d'être inclus dans un règlement de bons usages

119. Nous nous proposons de mentionner ici quelques éléments qu'une politique d'utilisation des outils informatiques est susceptible de contenir. Il est certain que plus une politique sera connue et acceptée par les travailleurs, plus elle sera susceptible d'être respectée et suivie par ces derniers. Bien que l'employeur doive parfois inclure dans ses directives un certain nombre de mentions obligatoires[222], le contenu de la charte dépendra fortement de la culture d'entreprise, de la sensibilité des informations traitées dans l'entreprise et des outils informatiques mis à disposition des employés[223].

1. Utilisation générale des outils informatiques

120. Cette liste exemplative sera à adapter, modifier ou compléter en fonction des souhaits de l'employeur, de la nature des activités du travailleur et de la culture d'entreprise[224].

- Imposition de mesures de sécurité (utilisation et changement de mots de passe) ;
- Précision selon laquelle chaque membre du personnel est responsable de son propre compte et ne peut en aucun cas laisser un tiers accéder à son *login* et son mot de passe ;
- Interdiction d'installer un quelconque programme ou logiciel, ou *hardware* sans autorisation de l'employeur ;
- Interdiction d'utiliser les outils informatiques à des fins personnelles, de les emmener au domicile, ou de sortir avec le matériel informatique sans autorisation de l'employeur ;
- Interdiction de désactiver l'antivirus ou le *firewall* ;

---

222 Rappelons que la C.C.T. n° 81, lorsqu'elle s'applique, requiert qu'un certain nombre d'informations figure sur ce document.

223 Nous renvoyons également à R. Blanpain et M. van Gestel, *Gebruik en controle van e-mail, intranet en internet in de onderneming, Praktijk en recht*, Bruges, Die Keure, 2003. Cet ouvrage aborde de manière très pratique l'élaboration d'une politique d'utilisation des outils de communication électronique.

224 Notons que les accès à certaines données en entreprise sont de plus en plus fréquemment divisés en *role-based access*, dont l'étendue dépend de la fonction que le travailleur occupe, et *rule-based access*, étant des accès déterminés en fonction du profil du travailleur (administrateur, assistant, directeur, etc.). Il est donc possible d'ériger plusieurs politiques d'accès différentes en fonction des profils de travailleurs concernés.

- Obligation de réaliser des *backups* réguliers des données stockées sur un PC portable ;
- Interdiction d'utiliser les ressources informatiques pour rédiger ou envoyer des courriers électroniques ou pour utiliser l'internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment l'envoi de messages ou la consultation de sites à caractère érotique ou pornographique, révisionniste, prônant la discrimination notamment sur la base du sexe, de l'orientation sexuelle, du handicap, de la religion, de la race ou de l'origine nationale ou ethnique, ou des convictions politiques ou religieuses d'une personne ou d'un groupe de personnes ;
- Interdiction de connecter du matériel à celui de l'entreprise ;
- Interdiction de copier ou transmettre des informations et données appartenant à l'entreprise ou des documents informatiques utilisés à des fins professionnelles sans que cette copie ou transmission ne concerne les activités habituelles du travailleur ;
- Interdiction de diffuser des informations confidentielles à l'extérieur ou de porter atteinte au mécanisme de sécurité mis en place pour les protéger ;
- Interdiction d'effectuer des actes illicites, tels que notamment le téléchargement de données ou œuvres protégées par un droit de propriété intellectuelle ;
- Interdiction d'utiliser le matériel de l'entreprise pour participer à une autre activité professionnelle ou à la recherche de gain ou d'un but de lucre pendant les heures de travail ;
- Interdiction d'exécuter des fichiers exécutables (.exe) vu le risque potentiel qu'ils représentent pour la sécurité de l'outil informatique et du réseau.

2. L'utilisation du courrier électronique

121. De manière non exhaustive, les règles relatives à l'utilisation du courrier électronique pourraient préciser les éléments qui suivent :

- Interdire l'usage de la messagerie professionnelle à des fins privées tout en tolérant l'utilisation d'une messagerie privée via le matériel de l'entreprise.
- En cas d'autorisation ou de tolérance de l'usage de la messagerie professionnelle pour un usage privé, plusieurs précisions peuvent être apportées. Par exemple :
  - mentionner que cet usage doit être occasionnel ;
  - autoriser un usage pour de courts messages uniquement ;

- omettre toute référence ou signature au nom de l'entreprise, ou toute autre indication qui pourrait faire croire que le message est rédigé par le travailleur dans le cadre de ses fonctions ;
- utilisation de préférence pendant les heures de pause ou hors des heures de bureau ;
- ne pas entraver la productivité ou la bonne conduite de l'entreprise ;
- ne faire aucune utilisation prohibée par la charte informatique de l'entreprise ;
- préciser que le message est privé en le mentionnant explicitement dans le champ 'sujet'.

– De manière générale, d'autres principes peuvent être prévus, comme par exemple :
  - une règle concernant la taille maximum des messages et leur contenu ;
  - l'obligation d'envoyer un accusé de réception lors de la réception d'un message par l'employé ;
  - l'obligation d'activer un message automatique de réponse (« *out of office* ») dans certaines circonstances ;
  - l'interdiction de dépasser telle capacité ou d'envoyer certains types de fichiers joints (fichiers videos, musicaux,…) ;
  - interdiction d'envoyer des courriers électroniques non sollicités (« *spamming* »), à caractère commercial, ou de participer à des chaînes de messages ;
  - interdiction de retransmettre des e-mails professionnels en l'absence de but professionnel légitime, dans des circonstances qui peuvent porter préjudice à l'entreprise ou à l'auteur du message originel ;
  - interdiction d'échanger des messages sans rapport avec la fonction exercée (textes, blagues, images, vidéos,…) vu les risques importants que représente cette pratique (blocage des sites, virus,…) ;
  - interdiction d'utiliser l'adresse e-mail à des fins de messagerie instantanée (ICQ, MSN,..) ou sur des cartes de visite personnelles ou tout autre document non professionnel.

3. Utilisation de l'internet

122. L'utilisation de l'internet peut être tolérée, mais devra dans ce cas respecter plusieurs principes, comme par exemple :

– l'interdiction de consulter des sites de certaines natures (commerciaux, pornographique, érotiques, sites de jeux, banque en ligne, téléchargement, sites faisant l'apologie de la discrimination notamment sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, des convictions

philosophiques ou politiques d'une personne ou d'un groupe de personnes, etc.) ;
– l'interdiction de participer à des forums de discussion ;
– l'interdiction d'utiliser certains programmes (Skype, MSN, etc.) ;
– l'interdiction d'accéder au *streaming*, musique ou vidéo en temps réel.

Par ailleurs, il est précisé que :
– l'employeur peut se réserver le droit de bloquer l'accès à certains sites et les mentionner dans le règlement ;
– l'accès à internet ne peut s'effectuer que sur le compte propre de l'utilisateur (ce qui peut se traduire par une interdiction de donner son *login* et mot de passe à un tiers) ;
– aucune activité interdite en vertu de la charte ne peut avoir lieu en utilisant l'internet.

C. Support de la règlementation

123. Il n'existe aucune exigence légale qui imposerait à l'employeur de définir les règles d'utilisation des outils informatiques et de communication dans un règlement de travail.

L'employeur est relativement libre de choisir le support sur lequel il établira son règlement d'utilisation ainsi que la forme que cette règlementation prendra. Aussi ces règles peuvent-elles être édictées dans un document informel tel qu'un « Règlement d'utilisation des outils informatiques », « Charte d'utilisation des moyens de communication électronique », ou encore « *IT Policy* ». Il peut être porté à la connaissance des travailleurs soit par la remise d'une copie, d'un envoi par e-mail ou encore d'une publication sur l'intranet de l'entreprise.

Ceci étant, il conviendra d'être attentif au fait que les règles du contrôle du respect de ces règles est quant à lui soumis à certaines exigences comme il sera expliqué dans la section 3.

Section 3
La mise en place d'une politique de contrôle

A. Principes généraux

124. Règlementer l'utilisation des outils informatiques sans pouvoir contrôler le respect de celle-ci risque d'en compromettre l'effectivité. Ceci dit, l'établissement d'une politique d'utilisation et de contrôle des moyens de communication électronique peut toutefois servir plusieurs objectifs. La politique aura un rôle d'information et de prévention, dès lors qu'elle visera à permettre aux

travailleurs d'assimiler les standards professionnels que l'on attend d'eux et à les empêcher de poser des actes contraires aux pratiques prohibées par l'employeur. La politique ainsi définie aura également un rôle d'avertissement, dès lors que chacun aura été informé des moyens de contrôle informatique mis en place, de leur raison d'être et des sanctions prévues en cas d'abus[225].

125. Il appartient à l'employeur de déterminer la politique de contrôle qu'il compte mettre en œuvre. Ce faisant, il devra rester attentif aux restrictions et conditions qui peuvent être posées aux contrôles envisagés. Nous nous proposons d'en aborder quatre : contrôle de l'usage de l'internet et de l'e-mail, accès à des fichiers stockés sur disque dur, géolocalisation et contrôle de l'usage du téléphone. Notons que, dans le cadre de la géolocalisation, c'est plutôt l'utilisation de cet outil à des fins de contrôle qui retiendra notre attention.

126. Dès lors que la mise en œuvre des contrôles envisagés entraîne une ingérence dans la vie privée des travailleurs et implique le traitement de données à caractère personnel des travailleurs, il appartiendra à l'employeur de respecter certains principes. Nous nous proposons de les aborder sous l'angle des quatre principes résultant de l'article 8 de la C.E.D.H. et que traduisent également les dispositions de la loi du décembre 1992. Cela constituera donc le minimum des règles à garder à l'esprit pour les quatre types de contrôles mis en place (section B, *infra*).

Après avoir rappelé les principes généraux qui s'appliquent à tout contrôle, nous nous attacherons à synthétiser les principes à respecter selon les types de contrôles envisagés (contrôle de l'usage de l'internet et de l'e-mail, accès à des fichiers stockés sur disque dur, géolocalisation, contrôle de l'usage du téléphone) (section C, *infra*).

Enfin, nous reviendrons sur les informations qui doivent figurer dans le document décrivant la politique à l'intention du personnel avant d'examiner si cette information doit se présenter sur un support spécifique (contrat de travail, règlement de travail, note interne,…) (section D, *infra*).

B. Les limites du contrôle face aux législations relatives à la protection de la vie privée

127. Pour rappel, l'article 8 de la C.E.D.H. et 22 de la Constitution permettent des ingérences dans la vie privée sous réserve du respect des principes de finalité, de proportionnalité, de légalité et de transparence[226].

---

225 Voy. « Une charte informatique… comment la créer et la mettre en place ? », http://easi.wallonie.be/servlet/Repository/EtudeCourrielRW_partie4_Charte.pdf ? IDR=8591.

226 Pour une analyse approfondie et l'application de ces principes en droit du travail, voy. F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, pp. 40-53 ; voy. ég. Th. Claeys N. Toussaint et D. Dejon-

Nous proposons d'exposer ici les principes généraux qui s'appliquent à tout contrôle, à la lumière de quatre principes susmentionnés. Nous verrons ensuite dans la section C, les implications concrètes de ces principes par rapport à certains modes de communication.

1. Les principes de légalité et de transparence

128. Ce sont souvent les principes de légalité et de transparence qui fonderont l'obligation pour l'employeur de déterminer dans un texte quelles sont les modalités de contrôle qu'il entend mettre en œuvre à l'égard du travailleur, ce dernier pouvant se prévaloir de la protection accordée par l'article 8 de la C.E.D.H. qui reçoit une application horizontale, également sur le lieu de travail[227].

a. Le principe de légalité

129. Comme expliqué *supra* sous la section 2, B du chapitre 2, l'article 8 de la C.E.D.H. reçoit une application horizontale en droit belge. Ceci implique que, dans les relations de travail, des ingérences peuvent intervenir dans le respect des conditions fixées par cette disposition.

L'obligation de légalité, nous l'avons vu, impose que l'ingérence dans la vie privée du travailleur soit prévue par une règle claire et précise accessible au travailleur, de façon à ce qu'il puisse prévoir les suites et adapter son comportement en conséquence[228].

L'exigence de légalité imposée par l'article 8 C.E.D.H. peut être rencontrée non seulement par l'intervention du législateur mais également par le biais d'une réglementation interne, pourvu qu'il s'agisse de normes claires et accessibles aux personnes concernées[229]. Ainsi, l'exigence de légalité nous semble pouvoir être atteinte au moyen de tout un arsenal de sources juridiques susceptibles de s'appliquer dans les relations de travail[230]. L'article 51 de la loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions

---

GHE, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2001, pp. 262-273.

227 Deux décisions récentes de la Cour du travail de Mons le rappellent : C. trav. Mons, 18 février 2008, *R.D.T.I.*, 2008, nº 31, p. 229 et C. trav. Mons, 22 mai 2007, *R.D.T.I.*, 2008/31, p. 239 ; voir également développements *supra*, chapitre 2, section 2, B, 1, b).

228 H. BARTH, « Contrôle de l'employeur de l'utilisation « privée » que font ses travailleurs des nouvelles technologies de l'information et de communication au lieu de travail », *J.T.T.*, 2002, p. 173.

229 Voy. *supra*, chapitre 2, section 2, B, 1.

230 Pour une analyse très complète des règles susceptibles d'intervenir dans les relations de travail pour limiter la vie privée des travailleurs, voy. F. HENDRICKX, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, pp. 115-127.

paritaires fournit une liste de ces sources, allant de la loi aux usages, en passant par la convention collective, individuelle, le contrat de travail, ou encore le règlement de travail. Il nous semble donc que les tribunaux pourront s'y référer et les considérer comme des lois au sens de l'article 8 C.E.D.H. à condition qu'elles soient suffisamment accessibles et précises[231].

130. Notons le cas particulier du règlement de travail, qui semble être, comme le relève J.-Fr. Neven, « la voie royale » qui rencontrerait les exigences du principe de légalité. Malgré quelques questions qui se posent[232], il n'en reste pas moins que ce mode de réglementation de l'usage et du contrôle de l'outil des moyens de communications électroniques semble la plus évidente dans le cadre juridique actuel[233].

Rappelons également que la C.C.T. nº 81 mentionne, à titre indicatif, que l'information qui doit être donnée aux travailleur pourra être réalisée :

- dans le cadre d'instructions générales (circulaires, affichage, etc.) ;
- par mention dans le règlement de travail ;
- par mention dans le contrat de travail individuel ;
- 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).

Le commentaire des articles 7 et 8 de la C.C.T. précise toutefois que ces dispositions ne dispensent pas, par ailleurs, de l'application de la réglementation en la matière, prévoyant des mentions obligatoires au règlement de travail comme, par exemple, en matière de sanctions.

Ceci étant, l'employeur ne peut bien entendu pas s'affranchir du cadre légal et prévoir des ingérences en contravention à la loi, et ce d'autant plus lorsque cette dernière prévoit précisément certaines limites à des ingérences

---

231 Voy. en ce sens ; J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-Fr. Leclerq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, p. 45, nº 35 ; F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, nºs 83-85, sur le principe de légalité et les nºs 115-127 sur les nuances apportées pour chaque type de texte analysé.

232 Le règlement de travail reçoit une place privilégiée comme instrument de régulation des relations de travail dès lors qu'il est une norme obligatoire consacrée par la loi du 5 décembre 1965 sur les conventions collectives de travail et les commissions paritaires ainsi que par la loi du 8 avril 1965 instituant les règlements de travail. Toutefois, si le règlement de travail est un moyen privilégié de réglementation de l'usage des nouvelles technologies, il n'en reste pas moins que sa force obligatoire pourra être remise en question dès lors qu'on se trouve face à une renonciation des droits fondamentaux du travailleur, laquelle devrait peut-être emprunter la voie d'une négociation individuelle (voir collective) pour être valable.

233 Voy. à ce sujet J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-Fr. Leclerq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, p. 45, nº 35 et les références citées.

telles celles prévalant en matière de prise de connaissance de communications électroniques ou de traitement de données à caractère personnel.

b. Le principe de transparence

131. On s'accorde généralement pour qu'il soit déduit de l'article 8 de la C.E.D.H. un devoir de transparence, corollaire de l'obligation de légalité : il s'agit de porter à la connaissance de l'individu concerné les ingérences potentielles ou effectives qu'il est amené à connaître[234].

L'exigence de transparence, ne résulte pas uniquement de l'article 8 précité. D'autres dispositions de droit belge impliquent également une exigence de transparence qui, soit se confond avec celle de l'article 8 C.E.D.H., soit porte sur les points distincts qui viendront s'y ajouter.

132. Nous pensons en particulier à la C.C.T. nº 81 qui énonce une série d'informations qui doivent être communiquées au personnel. Ces informations concernent les usages qui peuvent être faits des outils de communications électroniques, mais également des contrôles mis en place et des modalités de ceux-ci.

133. Cette obligation de transparence est également prévue à l'article 9 de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Cette disposition prévoit, en effet, que le responsable du traitement doit notamment informer les personnes concernées des finalités du traitement, des destinataires des données ou encore de l'existence d'un droit d'accès ou d'opposition[235]. Il s'agit d'une application

---

234 Th. Claeys, N. Toussaint et D. Dejonghe, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2001, p. 267 ; A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 35.

235 En vertu de l'article 9 de la loi, « Le responsable du traitement ou son représentant doit fournir à la personne concernée auprès de laquelle il obtient les données la concernant et au plus tard au moment où ces données sont obtenues, au moins les informations énumérées ci-dessous, sauf si la personne concernée en est déjà informée :

a) le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;
b) les finalités du traitement ;
c) l'existence d'un droit de s'opposer, sur demande et gratuitement, au traitement de données à caractère personnel la concernant envisagé à des fins de direct marketing ;
d) d'autres informations supplémentaires, notamment :
   – les destinataires ou les catégories de destinataires des données,
   – le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,
   – l'existence d'un droit d'accès et de rectification des données la concernant ; sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, ces

particulière du principe de transparence qui participe également au respect de l'article 8 C.E.D.H.[236].

134. Dans le cadre de son avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail[237], la Commission pour la protection de la vie privée a rappelé que, en vertu du principe de transparence, « le dialogue entre employeurs 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 »[238].

On remarque donc que les informations que la Commission recommande d'inclure dans la politique de contrôle ne concernent pas que les données à caractère personnel qui sont collectées, mais aussi l'utilisation des outils informatiques qui sont mis à sa disposition, ou encore les modes de contrôle qui sont mis en place par l'employeur.

Dans le même sens, le Groupe de travail de l'Article 29 suggère de rédiger une politique d'utilisation de l'internet[239]. En effet, le groupe de travail confirme que l'obligation de fournir des informations à la personne concernée constitue probablement « l'exemple le plus pertinent du principe de transparence ». Selon le document de travail du Groupe de l'Article 29, l'employeur doit fournir à son personnel « une déclaration claire, précise et aisément acces-

---

informations supplémentaires ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données ;

e) d'autres informations déterminées par le Roi en fonction du caractère spécifique du traitement, après avis de la commission de la protection de la vie privée. »

236 Pour plus de détails au sujet de l'obligation d'information visée à l'article 9 de la loi du 8 décembre 1992, voy. notamment B. Docquir, *Le droit de la vie privée*, Bruxelles, Larcier, 1998, pp. 185 et s.

237 Commission de la protection de la vie privée, Avis d'initiative n° 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommision.be.

238 Ces caractéristiques devront notamment viser :

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

239 Groupe de l'Article 29, document de travail, concernant la surveillance des communications électroniques sur le lieu de travail, 5401/01/FR/Final WP 55, adopté le 29 mai 2002, disponible à l'adresse http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf.

sible de sa politique relative à la surveillance du courrier électronique et de l'utilisation de l'internet »[240].

Nous reviendrons sur cette question *infra* sous le point F pour envisager plus avant les différents supports de communication et les informations qui devront concrètement être fournies.

2. Le principe de finalité

135. Pour être acceptables, les ingérences dans la vie privée doivent répondre à une exigence de finalité : la finalité doit être légitime et expressément annoncée[241].

Cela signifie notamment que l'ingérence dans la vie privée d'autrui doit s'effectuer en vue d'atteindre un des objectifs légitimes. Ainsi, ces finalités doivent rencontrer les critères avancés par l'article 8, § 2 de la C.E.D.H. À ce titre, on peut citer la protection des droits et libertés d'autrui, la nécessité de se

---

240 Selon le document de travail du Groupe de l'Article 29, « les salariés doivent être informés de façon complète sur les circonstances particulières qui justifieraient une telle mesure exceptionnelle ; ils doivent également être avertis de la portée et du champ d'application de ce contrôle. Il conviendrait notamment de leur communiquer :

1. les lignes directrices de l'entreprise concernant l'utilisation du courrier électronique ; elles doivent décrire dans le détail dans quelle mesure les systèmes de communication de l'entreprise peuvent être utilisés à des fins privées ou personnelles par les salariés (par exemple les limites concernant les périodes et la durée d'utilisation) ;
2. les motifs et les finalités de l'éventuelle mise en place d'une surveillance ; lorsque l'employeur a autorisé les salariés à utiliser les systèmes de communication de l'entreprise à des fins personnelles, les communications privées ne peuvent être surveillées que dans des cas très limités, p. ex. pour assurer la sécurité du système d'information (détection de virus).
3. des informations détaillées sur les mesures de surveillance prises, p. ex. qui ? quoi ? comment ? quand ?
4. des informations détaillées sur les procédures d'application précisant comment et quand les salariés seront avertis en cas d'infraction aux lignes directrices internes et pourront réagir dans un tel cas. Un autre exemple du principe de transparence est la pratique des employeurs qui consiste à informer et/ou consulter les représentants des salariés avant d'introduire des politiques les concernant ».

Le document précise en outre que « les décisions relatives à la surveillance des salariés, notamment le contrôle de leurs communications électroniques, sont couvertes par la récente directive 2002/14/CE, pour autant que l'entreprise concernée figure dans son champ d'application. En particulier, cette directive prévoit d'informer et de consulter les salariés concernant les décisions susceptibles d'entraîner des changements importants dans l'organisation du travail ou dans les relations contractuelles. La législation nationale ou des conventions collectives de travail peuvent énoncer des dispositions, davantage favorables aux salariés ».

241 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 36 ; Th. Claeys, N. Toussaint et D. Dejonghe, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2001, p. 265 ; CNIL, *Guide pratique pour les employeurs*, octobre 2005, p. 1, disponible sur www.cnil.fr.

préserver contre les infractions pénales, ou encore la protection de la morale, comme des objectifs légitimes répondants au prescrit de la C.E.D.H.[242].

Là encore, il y a toutefois lieu de se référer également aux lois particulières susceptibles de s'appliquer.

136. La loi du 8 décembre 1992 prévoit en son article 4, § 1, 2° que les données traitées doivent être 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.

Non seulement la finalité doit être légitime, mais elle doit également être annoncée, afin de pouvoir, d'une part, vérifier sa légitimé, mais aussi vérifier, d'autre part, qu'aucun détournement de finalité n'ait lieu. En effet, des données traitées en vue d'une finalité ne pourront pas l'être pour poursuivre d'autres finalités non annoncées conformément à l'article 9 de la loi (qui oblige d'informer les personnes concernées d'un ensemble d'éléments obligatoires concernant le traitement effectué).

137. Notons que la loi prévoit, en son article 5, plusieurs cas dans lesquels le traitement des données sera autorisé. Ainsi, ce traitement pourra être effectué avec le consentement de la personne, ou encore lorsqu'il est nécessaire à l'exécution d'un contrat, ou lorsqu'il est imposé par la loi, un décret ou une ordonnance.

En dehors des cinq cas dans lesquels le traitement sera autorisé (voir *littera* a à e de l'article 5 de la loi), l'article 5, f, dispose que les données peuvent être traitées lorsque cela 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.

Il s'agira donc d'opérer une balance des intérêts en présence pour apprécier la licéité du traitement. Celle-ci devra se faire entre la finalité poursuivie par l'employeur[243] et les intérêts de l'employé[244].

---

242 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 43; Th. Claeys, N. Toussaint et D. Dejonghe, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2001, p. 265.

243 La finalité pourra éventuellement être commerciale. Il nous semble toutefois que les intérêts moins impérieux sont moins susceptibles de justifier une ingérence dans la vie privée des travailleurs.

244 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, pp. 43-44. Les intérêts des tiers et des collègues pourront également être pris en compte : voy. *ibidem*, pp. 48 à 50.

138. On rappellera toutefois que la C.C.T. nº 81 énonce limitativement en son article 5 les motifs pour lesquels un contrôle des communications électroniques peut être instauré : seules ces finalités pourront justifier un contrôle tombant sous le champ d'application de la convention.

En outre, l'article 5, § 2 de la C.C.T. précise que l'employeur doit définir clairement la ou les finalités poursuivies dans son commentaire. Ceci permet d'éviter le détournement de finalités, puisque conformément à la loi du 8 décembre 1992, le traitement des données devra être conforme à cette finalité et si l'individualisation se fait dans le cadre d'une autre finalité, il devra être compatible avec celle initialement poursuivie par l'employeur[245].

139. Il en résulte que les données ne pourront pas être utilisées à d'autres fins que celles annoncées. On comprend donc l'importance de l'information préalable concernant la finalité poursuivie, dès lors qu'en l'absence d'une telle information, il sera impossible de vérifier que les données traitées le sont bien pour poursuivre les finalités initialement prévues.

3. Le principe de proportionnalité

140. Le droit de contrôle de l'employeur doit être exercé de la manière la moins dommageable possible lorsqu'il est susceptible d'entraîner une ingérence dans la vie privée du travailleur[246].

De ce principe, découlent plusieurs conséquences en ce qui concerne les modalités de contrôle.

141. Le principe de proportionnalité commande tout d'abord à l'employeur qu'il opte pour le contrôle qui implique le moins d'ingérence dans la vie privée du travailleur[247]. Cela suppose que, si des moyens non intrusifs sont disponibles pour atteindre une même finalité, ils devraient être privilégiés. Doivent ainsi être préférées les solutions qui limitent le plus possible l'ingérence dans la vie privée des travailleurs[248]. Comme mentionné ci-avant, l'utilisation de moyens techniques limitant l'accès à certains sites ou services, par exemple, sera

---

245 Voir rapport préliminaire de la C.C.T. nº 81.

246 Voy. par exemple « Document de travail du groupe de travail "article 29" concernant la surveillance des communications électroniques sur le lieu de travail », adopté le 29 mai 2002, 5401/091/FR/WP 55, p. 18, disponible à l'adresse http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf.

247 S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Éd. du Jeune Barreau de Bruxelles, Bruxelles, 2005, pp. 170-171.

248 A. REVEILLON, « La e-surveillance des employés. Le contrôle des *e-mails* et des sites visités », *Ubiquité*, 2002, nº 11, p. 43. Selon l'auteur, « Le moyen utilisé ne sera pas admis si des moyens moins nuisibles pouvaient réaliser les même objectifs ». Voy. également J.-Fr. NEVEN, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-F. LECLERQ (dir.), *Vie privée du travailleur et prérogatives*

ainsi préférée aux moyens principalement destinés à contrôler ou surveiller les comportements des travailleurs[249].

142. Les données à caractère personnel recueillies et traitées dans le cadre d'un contrôle doivent en outre être adéquates, pertinentes et non excessives au regard de la réalisation de l'objectif précisé. Le principe de proportionnalité est d'ailleurs rappelé par l'article 4, 3° de la loi du 8 décembre 1992[250]. Ainsi, il doit exister un lien de nécessité entre la collecte de données, le contrôle et la finalité poursuivie : l'ingérence doit être nécessaire et pas seulement utile pour réaliser la finalité[251]. Il conviendra d'adapter la politique de l'entreprise au type et au niveau de risques auxquels la société ou l'employeur est confronté[252]. À l'occasion du contrôle de proportionnalité, la balance des intérêts ne doit pas nécessairement s'opérer entre le droit à la vie privée du travailleur et d'autres droits fondamentaux : ainsi par exemple, les intérêts économiques de l'entreprise (protection contre la concurrence, sécurité de son matériel,…) peuvent être mis en balance avec le droit à la vie privée des travailleurs[253].

143. La Commission de la protection de la vie privée a quant à elle considéré que tout contrôle devrait être ponctuel et justifié par des indices laissant supposer une utilisation abusive des outils de travail[254]. La Commission exclut donc un contrôle général et *a priori* de l'ensemble des données de communication. La Commission considère d'ailleurs qu'il serait contraire à la dignité humaine de procéder à une surveillance constante des travailleurs.

En ce sens, la C.C.T. n° 81 prévoit que la surveillance doit être effectuée sur des données globalisées et que le contrôle ponctuel devra se réaliser en deux temps lorsque la finalité poursuivie est le contrôle du respect de la politique d'utilisation des outils de communication électronique par les travailleurs. Dans ce cas, la C.C.T. n° 81 interdit l'individualisation directe des données, c'est-à-dire sans avertissement préalable. De la même manière, l'audition du travailleur

---

patronales, Bruxelles, Éd. Jeune Barreau de Bruxelles, p. 31. En vertu de ce principe, une surveillance automatique continue sera souvent non justifiée et disproportionnée.

249 Groupe de l'Article 29, Document de travail concernant la surveillance des communications électroniques sur le lieu de travail, WP55, 29 mai 2002, http://ec.europa.eu/justice, p. 25.

250 Selon l'article 4 de la loi, « Les données traitées doivent être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement ».

251 F. HENDRICKX, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 44.

252 Groupe de l'Article 29, Document de travail concernant la surveillance des communications électroniques sur le lieu de travail, WP55, 29 mai 2002, http://ec.europa.eu/justice, p. 18.

253 Cass. 29 janvier 1999, *Bull.*, 1999, p. 111.

254 Commission de la protection de la vie privée, Avis d'initiative n° 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommision.be.

est rendue obligatoire avant de prendre toute sanction. L'article 14, § 2 de la C.C.T. précise d'ailleurs que les données individualisées doivent être adéquates, pertinentes et non excessives au regard de la ou des finalités poursuivie(s).

144. Une autre application du principe de proportionnalité concerne la durée de conservation des données. On notera que lorsqu'aucune obligation légale n'impose ou n'autorise la conservation de données (de trafic, de communication ou de localisation), la durée de conservation de ces données doit elle-même être proportionnée à la finalité poursuivie. En outre, le stockage des données pendant une durée déterminée (sur le serveur, par un *back-up* des *logs* ou par d'autres moyens) 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[255].

C. Synthèse des principes gouvernant la réglementation et le contrôle de l'usage de certaines technologies

145. Après avoir rappelé les différents principes généraux qui seront amenés à s'appliquer lors de tout contrôle, nous nous proposons ci-dessous d'examiner plus en détail la règlementation et le contrôle de certains outils de communication ou de technologies sujets à des spécificités qu'il nous paraît utile de souligner.

Nous analyserons successivement l'utilisation de la messagerie électronique et de l'internet, des données de géolocalisation et du téléphone pour terminer par l'analyse des fichiers stockés sur l'ordinateur du travailleur.

1. L'e-mail et internet

a. Dispositions applicables

146. Le contrôle de l'usage de l'e-mail et de l'internet peut s'analyser sous le même angle. En effet, l'utilisation de ces outils informatiques génère des communications électroniques qui sont protégées à la fois par le droit à la vie privée mais également par le secret des communications électroniques[256].

---

255 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, p. 6, www.privacycommission.be.

256 Document de travail du Groupe de l'Article 29 concernant la surveillance des communications électroniques sur le lieu de travail, 5401/01/FR/Final WP 55, adopté le 29 mai 2002, disponible à l'adresse http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf, p. 20. Le Groupe de l'Article 29 considère que « les communications électroniques émanant de locaux professionnels peuvent être couvertes par les notions de "vie privée" et de "correspondance" au sens de l'article 8, paragraphe 1 de la Convention européenne ».

Dès lors, outre le fait de rentrer dans le champ d'application des articles 8 de la C.E.D.H. et 22 de la Constitution, l'utilisation et le contrôle de l'e-mail et de l'internet relève de la C.C.T. nº 81 et est protégée par les dispositions légales relatives au secret des communications électroniques[257].

La loi du 8 décembre 1992 devra également être respectée. En effet, tant les e-mails que les données relatives à l'utilisation de l'internet constituent des données à caractère personnel dont le traitement automatisé entraîne l'application de la loi. En conséquence, l'employeur qui en contrôle l'usage sera considéré comme le responsable de traitement et devra déclarer le traitement de données à la Commission pour la protection de la vie privée, et respecter toutes les obligations qui pèsent sur le responsable de traitement en vertu de la loi.

b. Mise en œuvre du contrôle

§1er. Information à fournir aux employés

147. L'obligation d'information découle en particulier de l'article 9 de la loi du 8 décembre 1992. Dans le contexte d'un contrôle des communications électroniques du travailleur, la Commission pour la protection de la vie privée avait préconisé, conformément à l'article 9 de la loi du 8 décembre 1992, que le travailleur soit informé des différentes caractéristiques de la politique de contrôle de l'employeur à savoir :

> « - 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 »[258].

---

257 Voy. chapitre 2, section 3. Le secret des communications électroniques est assuré par les articles 314*bis* et 259*bis* du Code pénal et 124 et 125 de la loi du 13 juin 2005 sur les communications électroniques. Pour plus de développements sur le secret des communications électroniques, voy. P. De Hert, « Schending van het (tele)communicatie- geheim in het beroepsleven », *Rev. dr. soc.*, pp. 217 et s.

258 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

148. Le Groupe de l'Article 29 recommande quant à lui de communiquer aux travailleurs[259] :

« 1. les lignes directrices de l'entreprise concernant l'utilisation du courrier électronique ; elles doivent décrire dans le détail dans quelle mesure les systèmes de communication de l'entreprise peuvent être utilisés à des fins privées ou personnelles par les salariés (par exemple les limites concernant les périodes et la durée d'utilisation) ;
2. les motifs et les finalités de l'éventuelle mise en place d'une surveillance ; lorsque l'employeur a autorisé les salariés à utiliser les systèmes de communication de l'entreprise à des fins personnelles, les communications privées ne peuvent être surveillées que dans des cas très limités, p. ex. pour assurer la sécurité du système d'information (détection de virus).
3. des informations détaillées sur les mesures de surveillance prises, p. ex. qui ? quoi ? comment ? quand ?
4. des informations détaillées sur les procédures d'application précisant comment et quand les salariés seront avertis en cas d'infraction aux lignes directrices internes et pourront réagir dans un tel cas ».

149. Plus spécifiquement, concernant l'utilisation du courrier électronique, le Groupe de l'Article 29 considère qu'il y a lieu d'informer les travailleurs des points suivants :

« a) Déterminer si un salarié est autorisé à disposer d'un compte de courrier électronique à usage strictement personnel, si l'utilisation de comptes de messagerie web est autorisée sur le lieu de travail et si l'employeur recommande à son personnel l'utilisation d'un compte privé de messagerie web pour utiliser le courrier électronique à des fins strictement personnelles.
b) Les dispositions en vigueur prises avec les travailleurs concernant l'accès au contenu du courrier électronique, par ex. lorsque le travailleur est inopinément absent, et les finalités spécifiques de cet accès.
c) Signaler la durée de conservation des éventuelles copies de sauvegarde des messages.
d) Préciser quand les messages électroniques sont effacés définitivement du serveur.
e) Aspects de sécurité
f) L'implication de représentants de salariés dans la formulation de la politique. »[260].

---

259 Document de travail du Groupe de l'Article 29 concernant la surveillance des communications électroniques sur le lieu de travail, 5401/01/FR/Final WP 55, adopté le 29 mai 2002, disponible à l'adresse http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf, pt. 3.1.3.1.

260 Document de travail concernant la surveillance des communications électroniques sur le lieu de travail, adopté le 29 mai 2002, 5401/01/FR/Final, WP 55, disponible à l'adresse http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_fr.pdf, section 4.3.

150. En ce qui concerne spécifiquement la question de l'accès à internet, le Groupe de l'Article 29 considère qu'outre les informations à donner en vertu de l'obligation générale d'information, il convient d'aborder les points suivants :

> « - L'employeur doit préciser clairement aux salariés dans quelles conditions l'utilisation de l'internet à des fins privées est autorisée et leur indiquer les éléments qu'ils ne peuvent visualiser ou copier. Ces conditions et restrictions doivent être expliquées au personnel.
> - Les salariés doivent être informés des systèmes installés pour empêcher l'accès à certains sites ou pour détecter une éventuelle utilisation abusive. Les modalités du contrôle devraient être spécifiées, par exemple si ce contrôle est effectué de façon individualisée ou par service de l'entreprise ou si le contenu des sites consultés est visualisé ou enregistré par l'employeur dans certains cas. En outre, la charte doit spécifier, le cas échéant, l'usage qui sera fait des données collectées sur les personnes qui ont visité des sites spécifiques.
> - Les salariés doivent être informés du rôle de leurs représentants, tant dans la mise en œuvre de la charte que dans les enquêtes relatives aux infractions présumées »[261].

La C.C.T. nº 81 complète et précise cette obligation d'information, dès lors qu'elle indique les informations concernant les règles d'utilisation et les modalités du contrôle à communiquer aux travailleurs ; rappelons que cette information sera individuelle et collective[262]. On voit ici un lien entre la règlementation et le contrôle : aux termes de la C.C.T., les contrôles relatifs à des abus concernant l'utilisation faite des outils de communication impliquent au préalable que le travailleur ait été informé de ce qui est ou non permis dans l'entreprise.

§ 2. Les modalités du contrôle

151. Rappelons que la C.C.T. nº 81 avance quatre finalités qui seront considérées comme légitimes ainsi que la procédure à suivre pour un contrôle, faisant la différence entre individualisation directe et indirecte[263].

Comme la Commission de la protection de la vie privée l'a rappelé dans son avis 10/2000, le principe de proportionnalité commande que dans la majeure partie des cas, la prise de connaissance du contenu des informations n'est pas nécessaire à l'exercice du contrôle[264]. Dès lors, la prise de connaissance du contenu des courriers électroniques est excessive. En effet, il existe

---

261 *Idem,* section 5.2.

262 Voy. chapitre 2, section 5, B, 3 b).

263 Voy. art. 5 de la C.C.T. nº 81.

264 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

différentes solutions qui permettent de cibler les courriers suspects, comme des logiciels qui bloquent les chaînes d'e-mails ou les fichiers joints trop lourds.

La Cour du travail de Bruxelles a appliqué ce principe dans un cas d'espèce en considérant qu'il n'apparaissait pas que « la lecture du contenu de ces messages soit utile à la manifestation de la vérité et, dès lors n'est en jeu le droit au respect de la vie privée, la Cour considère, comme le Tribunal, que la production de la teneur de chaque message n'est en l'espèce ni nécessaire, ni indispensable, ni proportionné. »[265].

152. Rappelons que la C.C.T. nº 81 n'entend régir que le contrôle des données de communication et non le contenu de celles-ci. Il faudrait idéalement donc distinguer prise de connaissance des données et prise de connaissance du contenu, cette dernière ne pouvant être légitimée par le simple respect des modalités de contrôle de la CCT nº 81. Nous avons déjà souligné (voir chapitre 2, section 3, B *supra*) que cette distinction entre données relatives au contenu et données de communication n'est pas des plus aisée à cerner, faute de définition légale. Son application peut mener à quelques difficultés. En effet, il sera en pratique impossible pour l'employeur de faire abstraction de l'objet de l'e-mail concerné même s'il n'est pas exclu que l'objet de l'e-mail puisse être considéré comme relevant du contenu de celui-ci.

En outre, la C.C.T. nº 81 entend permettre à l'employeur de s'affranchir des restrictions qu'elle définit quant aux contrôles lorsque ceux-ci concernent des e-mails dont le caractère professionnel est non contesté. Comme nous l'avons évoqué *supra*[266], cet affranchissement nous paraît douteux au regard des dispositions légales qui s'appliquent indistinctement aux courriers privés et professionnels. Il nous paraît plus prudent dès lors d'inscrire tout contrôle portant sur des e-mails ou sur l'usage d'internet dans les modalités prévues par la C.C.T., indépendamment de la nature professionnelle ou privée des e-mails concernés.

153. En ce qui a trait au contrôle des sites internet consultés par l'employé, les données concernées sont les données de trafic, qui révèlent les adresses des sites consultés. Selon la Commission de la protection de la vie privée, il convient de considérer le contrôle portant sur ces données comme un traitement de données à caractère personnel. Le contrôle devra donc porter 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.

---

265 C. trav. Bruxelles, 22 novembre 2005, R.G. 46.320W, www.cass.be.

266 *Cf.* chapitre 2, section 5, B, 4.

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 ne soient identifiés dans un premier temps les auteurs des consultations[267].

Il devra, quoiqu'il en soit, respecter le prescrit de la C.C.T. nº 81 en ce qui concerne l'information préalable des travailleurs, mais aussi les procédures d'individualisation directes ou indirectes prévues par la C.C.T. Il ne pourra donc pas, par exemple, individualiser directement les données du trafic internet si la finalité du contrôle était le respect de la politique d'utilisation de l'internet au sein de l'entreprise.

§ 3. La nécessité d'obtenir le consentement de l'employé

154. Les articles 314*bis* et 259*bis* du Code pénal ainsi que l'article 124 de la loi du 13 juin 2005 sur les communications électroniques interdisent toute prise de connaissance d'une communication par un tiers à celle-ci sans le consentement de tous les participants à la communication[268].

Pour rappel, si les articles 314*bis* et 289*bis* du Code pénal ne visent que l'interception pendant la transmission de la communication, l'article 124 de la loi du 13 juin 2005 protège le secret des communications même après la transmission. Les e-mails seront donc protégés même après leur réception dans la boîte électronique de son destinataire.

Sauf à considérer que l'article 17 de la loi du 3 juillet 1978 constitue une base légale suffisante pour autoriser l'employeur à prendre connaissance des sites internet visités par ses travailleurs et des e-mails qu'il a envoyés ou reçus[269], le consentement du travailleur sera en principe requis.

155. Ce consentement doit être libre, spécifique et individuel. Rappelons qu'a déjà été questionné le caractère libre du consentement donné par un travailleur

---

267 La Commission préconise dans son avis que « l'employeur pourra par exemple disposer 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 levée de consultations 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 base de mots-clés déterminés ». (Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be).

268 Voy. chapitre 2, section 3.

269 Voy. *supra*, chapitre 2, section 3, B, 3, b).

à son employeur[270]. Par ailleurs, ce consentement ne devrait en principe pas être anticipatif et donné de manière générale à l'employeur[271].

Nous avons également vu que le consentement devra être individuel. Le consentement acté dans un règlement de travail ou une convention collective sera donc non valide. À cet égard, la Commission de la protection de la vie privée considère qu'il convient de combiner le consentement individuel de l'employé avec la négociation d'un texte général à laquelle seront associés les représentants des travailleurs[272]. On pourrait considérer que la C.C.T. nº 81, visant spécifiquement la problématique de la prise de connaissance des données de communication électroniques, constitue, en tant que résultat de concertation sociale, une base suffisante pour que le consentement du travailleur donné sur le contrôle de ses données de communication relatives à la navigation sur internet[273], suivant les modalités déterminées en application de la C.C.T., soit valide.

Le consentement de la personne pourrait être tacite. Subsiste alors toutefois la question de savoir dans quelles circonstances il pourra être admis que ce consentement a été donné de manière indubitable, mais également comment un consentement qui se déduit des circonstances pourra être considéré comme spécifique[274].

156. Enfin, il convient de rappeler que la loi exige l'obtention du consentement de toutes les personnes qui ont participé à la communication. En effet, aux termes de la loi, il convient non seulement d'obtenir le consentement valide du travailleur - ce qui n'est pas chose aisée - mais également de la personne (tierce ou non à l'entreprise) avec qui il a communiqué[275]. En pratique ce consentement sera presque impossible à obtenir. Certaines solutions ont été imaginées, comme par exemple la mention automatique sur tous les e-mails sortants de l'entreprise que les e-mails qui lui sont envoyés sont susceptibles

---

270 Commission de la protection de la vie privée, Avis nº 13/03 sur le contrôle par l'employeur des données de communication de l'un de ses employés, 27 février 2003, www.privacycommission.be, à propos du consentement d'un travailleur qui clique pour acceptation sur les conditions imposées par l'employeur pour l'utilisation de l'e-mail et de l'internet. Voy. aussi sur le consentement donné par une employée à la consultation de ses e-mails pendant un entretien : C. trav. Bruxelles, 13 septembre 2005, R.G. nº 46.114, www.cass.be.

271 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 197, pt. 322.

272 Commission de la protection de la vie privée, Avis nº 13/03 sur le contrôle par l'employeur des données de communication de l'un de ses employés, 27 février 2003, www.privacycommission.be.

273 Pour les données relatives aux e-mails, la question reste délicate puisqu'il faut l'accord de toutes les parties à la communication.

274 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 197, pt. 321. Rappelons toutefois l'arrêt déjà évoqué de la Cour du travail d'Anvers qui a constaté une autorisation « implicite » faite par une employée à un de ses collègues de consulter sa messagerie pendant son absence.

275 Sauf à déduire le consentement de ce participant des circonstances ; voy. P. Leduc, « Le contrôle des communications données et reçues par le travailleur », *Revue Ubiquité*, 2000/5, p. 48.

d'être lus par un collaborateur, sans que cela ne suffise toutefois à répondre à toutes les exigences de la loi[276].

157. L'application stricte de toutes les dispositions légales mentionnées, et notamment de l'interdiction d'intercepter des communications sans le consentement des deux parties, conduit à une impasse, ne serait-ce que lorsqu'on envisage la manière d'assurer la continuité du service en cas d'absence ou de départ des travailleurs.

En effet, l'accès aux e-mails des travailleurs sera le plus souvent indispensable en cas d'absence ou de départ de l'entreprise, par exemple pour assurer le suivi des commandes et des relations clients. Dans de tels cas, se pose la question de savoir si l'employeur peut, et à quelles conditions, accéder à la boîte e-mail du travailleur.

158. À cet égard, citons un arrêt de la Cour du travail de Liège, qui a admis la production des e-mails par l'employeur, au motif que celui-ci a licitement consulté ces messages à l'insu du travailleur dès lors qu'une convention préalablement souscrite par les parties visait à garantir le contenu purement professionnel de ceux-ci et permettait à l'employeur d'en prendre connaissance, quand l'intérêt de l'entreprise le requérait, sans l'autorisation préalable du travailleur et en dehors de la présence de celui-ci[277].

Dans une autre affaire, Belgacom avait relevé la boîte e-mail d'un salarié en son absence, après suspicion d'une utilisation non conforme à la police relative à l'utilisation de l'internet et de l'e-mail. Le Tribunal du travail de Mons a décidé que « le droit au respect de la vie privée sur les lieux de travail ne peut avoir pour effet d'exclure tout contrôle de l'employeur à propos du respect par le travailleur des obligations découlant de la loi sur le contrat de travail telles celles prévues à l'article 16 (de respecter les convenances et les bonnes mœurs pendant l'exécution du travail) ou à l'article 17 (d'exécuter le travail avec soin, probité et conscience, [...] et d'agir conformément aux ordres et instructions qui lui sont donnés).

---

276 La validité de ces solutions n'a à notre connaissance pas encore été soumise à un juge. Notons au passage l'arrêt du 22 novembre 2005 de la Cour du travail de Bruxelles qui considère que le contenu des messages échangés entre des employés de l'entreprise, même sur le lieu de travail, appartient à leur vie privée. Néanmoins, la Cour considère que l'employeur avait « le droit de contrôler, dans le respect des conditions de nécessité et de proportionnalité visées à l'article 8.2 de la C.E.D.H., l'emploi du temps de l'employé, ainsi que l'usage de la messagerie interne, y compris, dans une certaine mesure, le contenu des messages » ; voy. C. trav. Bruxelles, 22 novembre 2005, déjà cité.

277 C. trav. Liège, 26 avril 2010, R.G. nº 36389/09, www.cass.be.

À l'inverse, le droit de l'employeur de contrôler l'activité professionnelle de son travailleur ne peut priver celui-ci de la garantie du respect de sa vie privée[278].»

Ainsi, le Tribunal a estimé que le contrôle effectué par l'employeur n'enfreint pas le droit au respect de la correspondance lorsque [1] le travailleur est informé de l'éventualité d'un contrôle, [2] la finalité du contrôle répond aux objectifs de la loi et [3] la mesure de contrôle est proportionnée.

Ces principes pourraient être transposés au cas où la boîte aux lettres du travailleur est surveillée : il suffira alors d'informer les travailleurs qu'en leur absence, ou en cas de départ définitif de l'entreprise, leurs e-mails pourront être lus par une autre personne dans l'entreprise pour assurer la bonne continuité des activités de l'entreprise.

Ainsi, informer le travailleur de la possibilité d'un contrôle, ou d'un accès à sa boîte e-mail et des hypothèses dans lesquelles un tel accès pourra avoir lieu semble donc le minimum des précautions qui devront être prises par l'employeur.

159. Enfin, il convient de noter que le seul texte décrivant une procédure à suivre pour le contrôle des communications est la C.C.T. nº 81. L'organisation du contrôle telle que prévue par la C.C.T. ne mentionne pas l'exigence d'un consentement des personnes contrôlées, consentement toutefois exigé par l'article 124 de la loi du 13 décembre 2005. On ne peut donc que conseiller d'obtenir à tout le moins le consentement du travailleur, tout en gardant à l'esprit que le respect des dispositions de la C.C.T. nº 81 reste un standard minimal en deçà duquel l'employeur ne peut aller sans s'exposer à une méconnaissance flagrante des conditions de contrôle. La jurisprudence récente se limite en effet davantage à un contrôle au regard des principes de la C.C.T., laissant de côté l'examen des autres dispositions légales applicables ou la recherche d'un consentement du travailleur[279].

2. La géolocalisation

a. Dispositions applicables

160. Outre l'article 8 de la C.E.D.H. et 22 de la Constitution qui trouvent à s'appliquer dans la relation de travail, une disposition particulière concernant spécifiquement les données de localisation est insérée dans la loi du 13 juin 2005 relative aux communications électroniques.

---

278 Trib. trav. Mons, 28 juin 2010, R.G. nº 07/18715/A, www.cass.be.

279 Voy. K. Rosier, « Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *in Chronique de jurisprudence en droit des technologies de l'information (2002-2008)*, *R.D.T.I.*, 35/2009, p. 132, nº 217.

Il s'agit de l'article 123, § 1er qui dispose que « Sans préjudice de l'application 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, les opérateurs de réseaux mobiles ne peuvent traiter de données de localisation se rapportant à un abonné ou un utilisateur final que lorsqu'elles ont été rendues anonymes ou que le traitement s'inscrit dans le cadre de la fourniture d'un service à données de trafic ou de localisation »[280].

L'article 2, 7° de cette loi définit une donnée de localisation comme « toute donnée traitée dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur final d'un service de communications électroniques accessible au public ».

161. La sensibilité particulière de ces données a conduit le législateur européen à soumettre leur traitement à un régime spécifique qui impose notamment de recueillir le consentement de l'utilisateur ou de l'abonné préalablement au traitement de données de localisation et d'informer les personnes concernées des conditions de ce traitement (avoir article 123, § 2 de la loi du 13 juin 2005)[281].

Il résulte de ce qui précède que le traitement de données de géolocalisation par un opérateur implique l'obtention du consentement du travailleur, obtention dans laquelle l'employeur pourrait être amené à jouer un rôle.

162. Indépendamment de l'application de l'article 123 susmentionné, les données de géolocalisation se rapportant aux travailleurs seront en toute hypothèse soumises à la loi du 8 décembre 1992, laquelle régira le traitement des données

---

280 Voy. sur la notion de service à données de localisation, nº 76, *supra*.

281 L'article 123 § 2 dispose que « le traitement dans le cadre de la fourniture d'un service à données de trafic ou de localisation est soumis aux conditions suivantes :

1° L'opérateur informe l'abonné ou, le cas échéant, l'utilisateur final auquel se rapportent les données, avant d'obtenir le consentement de celui-ci pour le traitement :
   a) des types de données de localisation traités ;
   b) des objectifs précis du traitement ;
   c) de la durée du traitement ;
   d) des tiers éventuels auxquels ces données seront transmises ;
   e) de la possibilité de retirer à tout moment, définitivement ou temporairement, le consentement donné pour le traitement.

2° L'abonné ou, le cas échéant, l'utilisateur final, a préalablement au traitement, donné son consentement pour le traitement. Par consentement pour le traitement au sens du présent article, on entend la manifestation de volonté libre, spécifique et basée sur des informations par laquelle l'intéressé ou son représentant légal accepte que des données de localisation se rapportant à lui soient traitées.

3° Le traitement des données en question se limite aux actes et à la durée nécessaires pour fournir le service à données de trafic ou de localisation en question.

4° L'opérateur concerné offre gratuitement à ses abonnés ou à ses utilisateurs finals la possibilité de retirer le consentement donné, facilement et à tout moment, définitivement ou temporairement. »

de localisation effectué par l'employeur. L'employeur devra par conséquent non seulement notifier ce traitement à la Commission de la protection de la vie privée, mais également se conformer à la loi, en particulier, en ce qui concerne l'information à fournir aux travailleurs sur les finalités de ce traitement.

163. Outre l'application des textes mentionnés ci-dessus, on peut se demander si la portée large de la notion de « données de communication électroniques en réseau », telle qu'utilisée par la C.C.T. nº 81, n'entraîne pas l'applicabilité de cette convention collective au contrôle de données de localisation. En effet, le texte de la convention collective entend lui donner un champ d'application assez large (voir article 2 de la C.C.T. et son commentaire) et ces données transitent par réseau. Reconnaître que la C.C.T. nº 81 est applicable à la géolocalisation des travailleurs[282] par les employeurs restreindrait les finalités pour lesquelles les travailleurs pourraient utiliser les données de localisation, dès lors, par exemple, que le traitement de telles données à des fins d'optimisation du parc automobile par le biais de GPS ne rentre pas dans l'une des quatre finalités citées par la C.C.T.[283].

On peut regretter que le cadre que la C.C.T. nº 81, qui met clairement l'accent sur l'échange de courriers électroniques et l'utilisation d'internet, tout en affirmant son désir de respecter le principe de neutralité technologique, ne donne pas de précision à cet égard. Les auteurs n'examinent généralement pas cette question et semblent considérer que la C.C.T. nº 81 ne concerne pas la géolocalisation des travailleurs par leurs employés[284]. Il semble effectivement que la C.C.T. nº 81 n'ait, *a priori*, pas vocation à s'appliquer au contrôle des données de géolocalisation et que les données de localisation utilisées sortent du champ d'application de la C.C.T. nº 81 dès lors que celle-ci n'entend viser que les données de communication privées alors que les données de localisation sont supposées être professionnelles. En outre, les procédures décrites dans la C.C.T. nº 81 ont clairement été orientées vers le contrôle des e-mails et des sites internet (cela ressort notamment du principe de la procédure d'individualisation, ou des finalités mentionnées dans la C.C.T.).

---

282 En ce sens, voy. T. Messiaen, « Navigatiesysteem en privacy », *NjW*, nº 161, 2007, pp. 339-340.

283 Sauf à considérer que les données de localisation ne sont pas utilisées à des fins de contrôle, voir *supra*, chapitre 2, section 3, C. En outre, l'ensemble des autres prescriptions de la C.C.T devront être respectées.

284 Voy. O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, nº spécial 35 ans, mars 2005, pp. 45-46 ; A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 120 ; T. Messiaen cite la C.C.T. comme un texte potentiellement applicable à ce cas d'espèce mais sans en tirer de conséquences concrètes quant à son application : (T. Messiaen, « Navigatiesysteem en privacy », *NjW*, nº 161, 2007, pp. 339-340).

b. Mise en place d'un contrôle

164. Notons tout d'abord que contrairement aux autres contrôles envisagés, les moyens électroniques de géolocalisation ne sont pas en soi des instruments de travail, comme l'e-mail, l'internet ou encore l'ordinateur dont l'employeur entendrait vérifier l'usage. La seule fonction d'un terminal GPS pourra être de permettre de localiser un équipement, un travailleur ou un véhicule.

165. L'employeur devra informer le travailleur de la politique de traitement des données de localisation en vigueur. La Commission de la protection de la vie privée a émis un avis sur une proposition de loi sur le monitoring des données GPS des véhicules par les employeurs, mais ne donne pas beaucoup de précisions quant à ce qu'elle considérerait comme rencontrant les exigences de la loi[285].

Selon la CNIL[286], cette information devra porter sur l'identification des personnes soumises au contrôle, la nature des contrôles, les données concernées, et le destinataire des informations collectées[287].

Ainsi, le simple fait qu'un contrôle soit techniquement possible et concevable pour le travailleur ne suffit pas pour satisfaire à l'exigence de transparence. Aussi, c'est à tort, selon nous, que le Tribunal du travail de Liège semble avoir admis la connaissance de cette possibilité comme étant suffisante dans un litige où il avait à connaître d'une affaire où l'employé avait été licencié pour motif grave, notamment au motif qu'il s'était rendu chez une entreprise concurrente comme en attestaient les relevés GPS de son véhicule conservés par l'employeur[288]. Le Tribunal a considéré que les principes de finalité et de proportionnalité étaient respectés. Il semble en outre admettre que le principe de transparence n'empêchait pas l'admissibilité des éléments de localisation GPS produits par l'employeur au motif que « le défendeur savait que l'enregistrement GPS était possible ; que cet enregistrement a été effectué pour vérifier l'emploi du temps pendant le travail ». Or, le Tribunal relève dans son jugement que l'employeur n'informait pas ses travailleurs des relevés GPS enregistrés. On peut donc se demander si l'obligation de transparence, qui impose à l'employeur d'informer les travailleurs des surveillances éventuelles,

---

285 Voy. Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be.

286 « Commission nationale Informatique et Libertés », l'autorité française de protection des données.

287 Voy. Délibération n^{os} 2006-066 du 16 mars 2006 portant adoption d'une recommandation relative à la mise en œuvre de dispositifs destinés à géolocaliser les véhicules automobiles utilisés par les employés d'un organisme privé ou public, www.cnil.fr.

288 Trib. trav. Liège, 16 mai 2007, R.G. n° 358.538, www.cass.be.

est respectée. Il ne suffit pas selon nous que le travailleur sache qu'une surveillance est possible dans l'absolu ; encore doit-il être informé qu'elle est effectivement mise en place. En outre, le jugement semble considérer que le principe de finalité est respecté, mais ne mentionne pas l'objectif poursuivi par l'employeur qui enregistrait les données GPS de ses travailleurs à leur insu. Ces éléments nous paraissent être des faiblesses dans le raisonnement du Tribunal face aux principes exposés ici. En outre, le Tribunal n'a pas examiné la licéité du contrôle au regard des articles 123 et 124 de la loi du 13 juin 2005 (*cf. infra*, point c).

c. Le consentement du travailleur

166. Si le contrôle est réalisé par le biais d'un service à données de localisation, l'article 123 de la loi du 13 juin 2005 requiert d'informer et d'obtenir le consentement de l'abonné ou, le cas échéant, de l'utilisateur final, avant que l'opérateur ne traite des données de localisation. Cette disposition ne s'appliquera évidemment que si les données de localisation transitent par un réseau ou service de communication électronique et sont traitées par un opérateur, c'est-à-dire si les données de localisation ne sont pas générées automatiquement par le terminal lui-même (et donc sans utiliser les services d'un opérateur de communications électroniques, par exemple lorsque le téléphone portable est doté d'un dispositif de localisation par wi-fi)[289].

Si le texte de l'article 123 mentionne explicitement que c'est l'opérateur qui doit fournir l'information en question, il reste muet sur l'identité de la personne qui doit recueillir le consentement de l'utilisateur final. On pourrait imaginer que ce consentement soit obtenu par l'opérateur, le fournisseur de services à données de localisation ou encore l'employeur qui pourra être l'intermédiaire privilégié entre l'opérateur et le travailleur, utilisateur final.

En effet, l'article 123 requiert le consentement de l'abonné (l'employeur, qui a souscrit à un contrat) ou, le cas échéant, de l'utilisateur final (le travailleur). Or, il sera parfois difficile pour l'opérateur ou le fournisseur de services à données de localisation de savoir si l'abonné et l'utilisateur final sont des personnes différentes, et peu aisé pour lui d'obtenir le consentement des travailleurs directement alors que ces derniers ne sont pas en contact direct avec lui.

---

289 En effet, on ne serait alors plus en présence d'une donnée de localisation au sens de l'article 2, 7° de la loi du 13 juin 2005, c'est-à-dire d'une donnée « dans un réseau de communications électroniques indiquant la position géographique de l'équipement terminal d'un utilisateur final d'un service de communications électroniques accessible au public » ; voy. également Groupe de l'Article 29, Avis 5/2009 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy, p. 6.

C'est pourtant ce que confirme le Groupe de l'Article 29 qui estime que, « dans le cadre d'un service destiné aux particuliers, le consentement doit être recueilli auprès de la personne concernée par les données, c'est-à-dire auprès de l'utilisateur de l'équipement terminal »[290].

167. Dans ce cas, on peut se demander si l'on peut encore exiger de la part de l'opérateur qu'il informe l'utilisateur final (qu'il ne connaît pas forcément) du traitement de ses données de localisation mais également qu'il obtienne le consentement de celui-ci.

Peu importe selon nous que ce consentement soit recueilli par l'opérateur, le fournisseur de services ou encore l'employeur. Un principe nous paraît cependant clair : la responsabilité d'obtenir un tel consentement en vertu de l'article 123 de la loi du 13 juin 2005 repose sur l'opérateur ou le fournisseur de services à valeur ajoutée traitant des données de géolocalisation.

168. Indépendamment de cette obligation d'information et de consentement à charge de l'opérateur ou du fournisseur de services à données de localisation, certains auteurs considèrent que le consentement spécifique de l'intéressé devrait être obtenu par l'employeur lorsque que ces données sont traitées dans le but de surveiller les déplacements des travailleurs par géolocalisation[291]. Deux bases juridiques peuvent être avancées.

D'une part, on peut considérer, comme O. Rijckaert, que le consentement de l'intéressé est requis en vertu de l'article 4 de la loi du 8 décembre 1992, dès lors que le traitement de données de géolocalisation n'est pas nécessaire à l'exécution du contrat de travail. En effet, selon l'auteur, « si tel était le cas, il faudrait en déduire que, préalablement à cette innovation technologique que constitue la géolocalisation, les contrats de travail des travailleurs itinérants ne pouvaient être exécutés correctement »[292].

---

290 Groupe de l'Article 29, Avis 5/2009 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy, p. 7.

291 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 56 ; A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 133. Le consentement serait donc requis même dans les cas où l'article 123 ne viendrait pas à s'appliquer.

292 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 56. L'auteur souligne que si les données relatives à l'identité et au domicile du travailleur sont nécessaires à l'exécution du contrat de travail, tel n'est pas le cas des données de géolocalisation : si elles permettent une meilleure organisation du travail, voire une meilleure exécution du contrat liant l'employeur à ses clients, elles ne sont en rien indispensables à l'exécution du contrat de travail en tant que tel ; *contra* : le Groupe de l'Article 29 considère quant à lui que le traitement peut être justifié lorsqu'il est effectué aux fins de la surveillance du transport de personnes ou de marchandises, d'une meilleure affectation des ressources pour des prestations à fournir en des lieux dispersés ou de la poursuite d'un objectif de sécurité. (Groupe de l'Article 29, Avis 5/2005 sur l'utilisation de données de

D'autre part, certains défendent l'idée qu'en vertu de l'article 124 de la loi du 13 juin 2005, qui interdit la prise de connaissance de communications électroniques concernant des tiers, le consentement du travailleur devra être obtenu par l'employeur[293]. Reste à savoir si l'exception prévue par l'article 125, concernant les cas où la loi autorise une telle prise de connaissance, peut trouver à s'appliquer en présence de l'article 17, 2° de la loi sur les contrats de travail, ce qui est controversé[294].

L'accord individuel des travailleurs semble nécessaire aux yeux de la Commission de la protection de la vie privée, mais également du Groupe de l'Article 29, notamment eu égard aux dispositions légales en matière de protection de la vie privée dans le secteur des communications électroniques (et ce, même dans les cas où les données de géolocalisation ne seraient pas générées par un opérateur et où l'article 123 de la loi du 13 juin 2005 ne s'appliquerait *a priori* pas)[295].

169. Concernant les modalités permettant d'assurer un consentement libre et spécifique, la Commission considère dans son avis 12/2005 que, dans les cas où cela s'avère être faisable, « la solution optimale consisterait à permettre à l'employé d'activer et de désactiver le système de façon ponctuelle, selon les nécessités de sa localisation (par exemple, à l'arrivée et au départ de chaque lieu où il doit se rendre). Le système devrait en tout état de cause pouvoir être désactivé lors de l'utilisation du véhicule en dehors des heures de travail »[296]. À cet égard, rappelons que l'article 123 de la loi du 13 juin 2005 dispose que « L'opérateur concerné offre gratuitement à ses abonnés ou à ses utilisateurs finals la possibilité de retirer le consentement donné, facilement et à tout moment, définitivement ou temporairement ».

Le consentement du travailleur pourra donc résulter de l'acceptation sur son terminal des conditions d'utilisation et de la possibilité de refuser temporairement sa localisation, notamment lorsqu'il effectue des trajets privés, le

---

localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy, p. 11).

293 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 133 ; *cf.* Avis 12/2005 précité du 25 novembre 2005 de la Commission de la protection de la vie privée, au sein duquel la Commission indique que l'accord individuel des travailleurs semble nécessaire, et notamment eu égard à l'article 123 de la loi du 13 juin 2005.

294 *Cf. supra* chapitre 2 ; section 3, B, 3.

295 Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be, n° 19.

296 *Ibidem*, p. 11.

tout après avoir été informé des conditions du traitement de ses données de localisation.

170. Toutefois, selon le Groupe de l'Article 29, la légitimité des opérations de traitement ne doit pas reposer exclusivement sur le consentement du travailleur[297]. Ceci implique que le Groupe estime que le recours à la géolocalisation doit par ailleurs reposer sur une finalité légitime. Concernant le consentement, l'avis du Groupe de l'Article 29 rappelle que celui-ci doit être une manifestation de volonté libre. À cet égard, le document signale que la question du consentement doit être envisagée dans une perspective plus large : l'implication de toutes les parties prenantes par le biais de conventions collectives pourrait ainsi, selon le Groupe de l'Article 29, constituer une façon adéquate de réglementer l'obtention des déclarations de consentement dans de telles situations.

C'est dans ce sens qu'allait la proposition de loi analysée par la Commission de la protection de la vie privée[298] : selon le texte examiné, le traitement de données à caractère personnel ne pouvait être effectué qu'après accord des commissions paritaires *ad hoc*, du comité commun à l'ensemble des services publics ou des organes compétents en vertu du régime des relations collectives de travail, en d'autres termes, moyennant l'accord des syndicats. La Commission précise que les différents textes imposant une consultation sociale[299] ne peuvent être considérés que comme des compléments à l'obligation d'information reprise à l'article 9 de la loi du 8 décembre 1992. En outre, la Commission estime que l'accord des syndicats, bien qu'il signifie dans ce cas un pas en avant, peut difficilement passer pour un consentement des personnes concernées.

171. Dès lors, l'obtention du consentement du travailleur, doublé d'une information sur le traitement de ses données de localisation et consolidée par une concertation sociale, nous paraît offrir le maximum de sécurité juridique pour assurer la licéité d'une surveillance des travailleurs sur base de leurs données de localisation[300].

---

297 Groupe de l'Article 29, Avis 5/2009 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy, p. 11.

298 Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be, nº 16.

299 Notamment : la recommandation R(89) du Conseil de l'Europe, le Code de conduite de l'Organisation internationale du Travail en matière de protection des données à caractère personnel des travailleurs de 1996, la loi du 20 septembre 1948 portant organisation de l'économie, la loi instituant les règlements de travail du 8 avril 1968, la C.C.T. nº 9 du 9 mars 1972, la C.C.T. nº 39 du 13 décembre 1984.

300 Le contrat de travail pourrait permettre de recueillir un tel consentement, même si on y trouve rarement une disposition concernant la géolocalisation du travailleur. Voy. T. Messiaen, « Navigatiesysteem en privacy », *NjW*, nº 161, 2007, p. 343.

Enfin, rappelons que, outre la question de l'obtention du consentement, les finalités de la prise de connaissance des données devront bien sûr répondre aux exigences de l'article 8 C.E.D.H. et de la loi du 8 décembre 1992, et notamment aux principes de transparence et de proportionnalité qu'ils consacrent.

d. Les modalités du contrôle

172. En application de la loi du 8 décembre 1992, tout traitement de données à caractère personnel, tel qu'un système permettant de rechercher la localisation précise des membres de son personnel, doit répondre à des finalités déterminées explicites et légitimes qui en justifient l'installation et l'utilisation.

La détermination de finalités est donc essentielle, et ce, d'autant plus que la loi du 8 décembre 1992 interdit le traitement de données à des fins incompatibles avec la finalité initialement envisagée.

C'est ce qu'a rappelé la CNIL à propos du détournement de finalité interdit par la loi : « l'utilisation des informations collectées par des dispositifs de géolocalisation doit correspondre à l'objectif déclaré et ne doit pas servir à d'autres fins. Ainsi, l'employeur qui utiliserait le dispositif de géolocalisation pour contrôler l'activité de ses employés alors que la finalité déclarée à la CNIL est la lutte contre le vol, commettrait un détournement de finalité. Le fait d'utiliser des données personnelles à des fins étrangères à celles qui ont justifié leur collecte est une infraction pénale »[301].

173. Selon O. Rijckaert, « des données de localisation originellement collectées en vue de faire face à une situation particulière, telle la demande urgente d'un client, ne pourraient pas par la suite être utilisées à des fins d'évaluation ou de sanction du travailleur »[302].

Au regard de ces principes, on peut remettre en cause la solution retenue dans un arrêt de la Cour du travail de Bruxelles qui a dû connaître d'un cas de licenciement pour motif grave suite à la constatation par l'employeur d'excès de vitesse récurrent à l'aide du GPS. La Cour a en l'espèce considéré que l'utilisation par une société de taxis de GPS en vue de pouvoir localiser ses véhicules et de permettre ainsi de diriger un taxi vers un client sur la base de la proximité ne portait pas atteinte à la vie privée du travailleur[303]. On peut critiquer ce jugement à deux points de vue, selon nous. D'une part, il nous

---

301 CNIL, *Guide de la Géolocalisation des salariés, Droits et obligations en matière de géolocalisation des employés par un dispositif de suivi GSM/GPS*, http://www.cnil.fr/fileadmin/documents/approfondir/dossier/geolocalisation/Guide-geolocalisation.pdf.

302 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 56.

303 C. trav. Bruxelles, 18 novembre 2004, *J.T.T.*, p. 145.

paraît clair, en vertu de la jurisprudence de la Cour européenne des droits de l'homme, que pareille surveillance constitue une ingérence dans la vie des individus, que celle-ci soit légitime ou non[304]. D'autre part, on constate que la finalité première qui semblait être la gestion du parc de taxis pour une intervention rapide de ceux-ci, a été détournée pour surveiller la vitesse des employés, sans que ceux-ci n'aient été informés de ce contrôle[305].

174. Quant aux finalités admissibles, la Commission de la protection de la vie privée a, à l'occasion de l'analyse d'une proposition de loi sur la question, identifié plusieurs finalités qui peuvent être poursuivies par l'employeur : la sécurité du travailleur, la protection des véhicules, des besoins professionnels bien définis concernant le transport et la logistique (gestion du parc automobile), ou encore le contrôle sur le travail de l'employé[306].

Le Groupe de l'Article 29 a pointé quant à lui que le traitement de données de localisation doit répondre à un besoin spécifique de l'entreprise, lié à son activité. Ce traitement peut donc être justifié lorsqu'il est effectué aux fins de la surveillance du transport de personnes ou de marchandises, d'une meilleure affectation des ressources pour des prestations à fournir en des lieux dispersés, ou de la poursuite d'un objectif de sécurité. Par contre, le Groupe de l'Article 29 précise que le traitement des données sera excessif si les travailleurs sont libres d'organiser leur travail comme ils l'entendent ou si le contrôle de leur travail constitue la seule finalité dudit traitement alors que ce contrôle pourrait être réalisé par d'autres moyens[307]. Cependant, cette appréciation relève plus, à notre avis, du principe de proportionnalité que de celui de finalité.

175. En outre, le traitement doit porter, conformément à la loi du 8 décembre 1992, sur des données adéquates, non excessives et pertinentes au regard des finalités poursuivies. Le Groupe de l'Article 29 rappelle, en cas de géolocali-

---

304 La Cour se place même sur le terrain de la proportionnalité pour se prononcer et considère que ce principe est respecté lorsqu'on met en balance la protection de la vie privée d'une part, et le droit de l'employeur et l'intérêt de la collectivité, d'autre part.

305 Pour une décision refusant de prendre en compte des données de géolocalisation obtenue dans avoir informé le travailleur préalablement de la possibilité du contrôle, voyez Cour d'appel de Dijon (Ch. sociale), 14 septembre 2010, *Mille Services c. Rémi X*, www.legalis.net.

306 Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be.

307 Groupe de l'Article 29, Avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy, p. 11.

sation des travailleurs, la nécessité de surveiller les travailleurs de la manière la moins intrusive possible[308].

Selon la Commission de la protection de la vie privée, si le traitement a pour but l'exécution des missions confiées aux travailleurs, pareil contrôle devrait être ponctuel et justifié par des indices faisant soupçonner des abus de la part de certains employés[309]. Outre les cas d'abus, le contrôle par l'employeur au moyen d'un système de géolocalisation sera permis s'il est effectué dans l'intérêt de la sécurité du travailleur.

176. Quoiqu'il en soit, un contrôle permanent, avec lecture systématique des données enregistrées, doit en principe être considéré comme disproportionné[310]. Toutefois, selon la CNIL, « si la mise en œuvre d'un dispositif de géolocalisation a généralement pour objectif de repérer immédiatement le véhicule le plus proche d'une demande "client", il peut également servir à surveiller les employés. À cet égard, la CNIL recommande que la surveillance des déplacements des employés ne soit pas permanente et ne puisse être mise en œuvre que si la tâche à accomplir réside dans le déplacement lui-même, ce qui est le cas par exemple des taxis »[311].

Dans le même esprit, la Commission de la protection de la vie privée estime qu'il existe des hypothèses dans lesquelles un contrôle plus régulier pourrait être justifié s'il est directement lié à la nature des tâches à accomplir par l'employé, comme l'optimisation de la gestion des déplacements des véhicules (vendeurs, techniciens de terrain,…). Dans ce cas, la Commission considère qu'un contrôle se déroulant tout au long de la journée peut être

---

308 Groupe de l'Article 29, Avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy, p. 10.

309 Voy. Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be, nº 22 ; selon O. Rijckaert, si on peut concevoir que l'employeur interroge ponctuellement le système de géolocalisation afin d'identifier rapidement le technicien le plus proche du site en question, ne répondrait pas à la condition de proportionnalité une surveillance constante des mouvements du travailleurs durant la journée de travail, par exemple, pour mesurer la rapidité ou l'efficacité de leurs déplacements. (O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, nº spécial 35 ans, mars 2005, p. 56).

310 Voy. Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be, nº 24. La Commission mentionne toutefois qu'un tel contrôle pourrait être envisagé pour des raisons de sécurité, dans un contexte spécifique, comme par exemple un transport nucléaire ou un transport de fonds.

311 CNIL, *Guide de la Géolocalisation des salariés, Droits et obligations en matière de géolocalisation des employés par un dispositif de suivi GSM/GPS*, www.cnil.fr.

admis, sans toutefois que ce contrôle soit continu[312]. La Commission ajoute que la solution optimale serait, selon elle, de permettre à l'employé d'activer et de désactiver le système de manière ponctuelle, selon les nécessités de sa localisation.

Toujours en application du principe de proportionnalité, le Groupe de l'Article 29 considère que le traitement devrait être par principe effectué en temps réel, sans conservation des données[313]. En tout état de cause, si l'objectif poursuivi pouvait justifier une conservation plus longue, le Groupe de l'Article 29 estime que la durée de conservation de ces données ne devra pas dépasser deux mois.

3. Les communications téléphoniques

a. Les principes applicables

177. Il est fréquent que l'employeur mette à la disposition d'un travailleur un téléphone et/ou un GSM de société. L'employeur pourra décider d'interdire complètement toute utilisation non professionnelle du téléphone ou, au contraire, tolérer voire même autoriser des appels non professionnels avec l'appareil mis à disposition. Dans ce cas, les appels au départ d'un téléphone fixe, ou d'un GSM, ainsi que les SMS ne pourront pas être effectués à des fins personnelles. Par ailleurs, dans un tel cas de figure, c'est bien souvent l'employeur qui sera l'abonné au service téléphonique et qui, de ce fait, recevra également les factures relatives à ces abonnements.

Nous avons déjà vu que les communications téléphoniques (incluant les appels et les SMS vers et au départ d'un GSM) sont, au travail comme ailleurs, protégées par les articles 8 de la C.E.D.H. et 22 de la Constitution[314]. La Cour européenne des droits de l'homme a d'ailleurs rappelé ce principe à plusieurs reprises, et notamment dans des cas relatifs à l'utilisation du téléphone sur le lieu de travail[315], en particulier dans son arrêt *Copland*[316]. Ceci vaut tant pour la prise de connaissance du contenu des communications que de celle des données de communication. La Cour de cassation a quant à elle estimé que «le repérage des communications téléphoniques, consistant à relever, à l'insu

---

312 Voy. Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be, nº 25.

313 Voy. CNIL, *Guide de la Géolocalisation des salariés, Droits et obligations en matière de géolocalisation des employés par un dispositif de suivi GSM/GPS*, www.cnil.fr, qui partage cette opinion.

314 Voy. *supra* chapitre 2, section 2, B.; voy. également Cass., 10 avril 1999, *Pas.*, I., p. 932.

315 C.E.D.H., 16 décembre 1992, *Niemietz c. Allemagne*, *J.T.T.*, 1994, p. 65; C.E.D.H., 27 mai 1997, *Halford c. Royaume-Uni*, *Rec.*, 1997 – III, p. 39.

316 C.E.D.H., 3 avril 2007, *Copland c. Royaume-Uni,* http://www.echr.coe.int/echr/.

de l'abonné, les numéros appelés et permettant ainsi d'obtenir des informations relatives aux numéros composés, qui font partie intégrante des communications téléphoniques, constitue une ingérence dans l'exercice du droit au respect de la vie privée, garantie par l'article 8 de la Convention »[317]. Par conséquent, nous ne pouvons partager l'avis de F. Lagasse et M. Milde, selon lesquels « l'employé ne pourrait se retrancher derrière le principe du respect de la vie privée pour réfuter le reproche qui lui serait formulé (éventuellement dans le cadre d'un licenciement) d'avoir "abusé" du téléphone de l'employeur »[318].

178. En outre, les différentes obligations énumérées par loi du 8 décembre 1992 devront être respectées dès lors que les données de téléphonie sont traitées par l'employeur. Ceci implique notamment l'obligation d'informer les travailleurs des modalités du traitement et de leur permettre d'exercer un droit d'accès et d'opposition[319].

Nous avons déjà évoqué que la C.C.T. nº 81 pourrait, *a priori*, également trouver à s'appliquer au contrôle de l'usage du téléphone. En effet, une conversation téléphonique est bien une communication électronique en réseau au sens de la C.C.T. nº 81[320]. Cela dit, nous avons de sérieux doutes quant à l'application de la C.C.T. nº 81 aux communications téléphoniques dès lors que les principes édictés par ce texte ne sont pas facilement transposables au contrôle des communications électroniques[321].

179. Rappelons que les dispositions relatives à l'interdiction de prise de connaissance des communications électroniques seront d'application (articles 314*bis* et 259 *bis* du Code pénal et 124 de la loi du 13 juin 2005, voy. *supra* chapitre 2, section 3, C). Il résulte de l'ensemble de ces dispositions que la prise de connaissance de communications téléphoniques sera impossible, sauf exceptions énumérées ci-dessous.

---

317 Cass., 23 janvier 1991, *J.L.M.B.*, 1991, p. 1420 ; Cass., 2 mai 1990, *J.T.*, 1990, p. 469.

318 F. Lagasse et M. Milde, « Protection de la personne et vie privée du travailleur : Investigation et contrôle sur les lieux de travail », *Orientations*, juin/juillet 1992, p. 151.

319 Pour rappel, la simple collecte, ou la simple détention de données relatives à l'usage du téléphone par l'employé sont susceptibles d'entraîner l'application de la loi du 8 décembre 1992.

320 À ce sujet, voy. S. van Wassenhove, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. Leclercq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. du Jeune Barreau de Bruxelles, 2005, p. 175 ; A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 133.

321 Chapitre 2, section 5, B, 2, b.

180. Ainsi, l'article 314*bis* du Code pénal interdit notamment les actes suivants :

> « 1° soit, intentionnellement, à l'aide d'un appareil quelconque, écoute ou fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications ;
>
> 2° soit, avec l'intention de commettre une des infractions mentionnées ci-dessus, installe ou fait installer un appareil quelconque.

L'utilisation d'un appareil est nécessaire pour que cette disposition s'applique. Il sera donc interdit pour l'employeur d'installer un appareil d'enregistrement des conversations des travailleurs. Par contre, la prise de connaissance de conversations sans utilisation de dispositif ne serait pas punissable sur pied de l'article 314*bis*[322].

Cette interdiction ne s'applique que pendant la transmission[323]. Elle ne s'adresse qu'aux tiers à la communication et ne protège que le contenu de la communication. Les travaux préparatoires de la loi du 30 juin 1994 insérant l'article 314*bis* du Code pénal, envisagent d'ailleurs la possibilité pour l'employeur de relever les numéros de téléphone appelés par ses travailleurs[324].

181. Quant à l'article 124 de la loi du 13 juin 2005, il reçoit un champ d'application plus large, puisqu'il concerne les données relatives aux communications électroniques, qu'il reste applicable même après la transmission de la communication électronique, et qu'il interdit, notamment, la prise de connaissance des données relatives aux communications électroniques. Ainsi, cette disposition s'applique aussi bien au contenu des communications qu'à leurs données satellites (l'heure d'appel, les numéros appelés, le nombre de SMS, etc.).

Nous l'avons vu, les dispositions applicables empêchent en principe l'employeur de prendre connaissance des données et du contenu des commu-

---

322 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 67. Suivre ce raisonnement permettrait à un tiers de prendre connaissance d'une conversation téléphonique via un autre terminal connecté à la conversation ayant lieu. On ne voit toutefois pas en quoi l'absence de dispositif d'écoute rend l'acte moins critiquable.

323 On peut toutefois s'interroger sur la prise de connaissance d'un message vocal sur un répondeur distant, ou d'un SMS non ouvert. À ce sujet, voy. A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 67.

324 Projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement des communications et de télécommunications privées, *Ann. Parl.*, Sén., 1992-1993, n° 843/2, p. 42.

nications téléphoniques des travailleurs[325]. Toutefois, certaines exceptions sont prévues par la loi et pourraient permettre à l'employeur d'en prendre licitement connaissance.

Ces exceptions sont les suivantes :

1. Consentement des personnes participant à la communication

182. Nous l'avons mentionné, le consentement de tous les participants à la conversation téléphonique sera requis pour que la prise de connaissance soit légale.

En ce qui concerne le consentement du travailleur, nous avons vu que ce dernier peut être implicite. Il devra néanmoins être exprès et libre. Cette dernière condition est parfois difficile à rencontrer pour un travailleur qui n'aura souvent d'autre choix que d'accepter la prise de connaissance de la communication faute de pouvoir utiliser le téléphone. Rappelons à cet égard qu'avant l'adoption de l'article 128 de la loi du 13 juin 2005, la Commission de la protection de la vie privée avait rendu des recommandations en la matière. Elle avait considéré, dans sa recommandation n° 1/2002 du 22 août 2002, qu'une note de service ou un règlement de travail n'étaient pas suffisants pour garantir le consentement libre de l'employé[326]. La Commission préconisait de combiner le consentement individuel avec la négociation d'un texte général auquel les représentants des employés seraient associés.

L'obtention du consentement de l'autre partie avec qui l'employé a communiqué sera dans tous les cas difficile à obtenir, et il sera en pratique rarement donné par le tiers avec qui le travailleur est entré en contact. La recommandation n° 1/2002 de la Commission de la protection de la vie privée proposait, pour ce qui est du consentement des clients de l'entreprise, que ce dernier puisse être obtenu à la signature des conditions d'utilisation du service téléphonique proposé (en l'espèce, un service téléphonique bancaire), à condition que le client ait été informé des conditions d'enregistrement des communications.

2. Autorisation légale

183. Nous avons vu que l'article 125 de la loi du 13 juin 2005 autorise la prise de connaissance d'informations transmises par voie de communications

---

325 Voy. *supra*, chapitre 2, section 3, B.

326 Voy. pour l'application de ces principes pour les services bancaires téléphoniques, la recommandation n° 1/2002 du 22 août 2002 de la Commission de la protection de la vie privée sur l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, www.privacycommission.be. Dans un même ordre d'idées, le recours à un dispositif « Zoller », par exemple, sera disproportionné pour surveiller l'activité d'un travailleur (F. Lagasse et M. Milde, « Protection de la personne et vie privée du travailleur. Investigation et contrôle sur les lieux du travail », *Orientations*, 1992, p. 153).

électroniques lorsqu'une loi autorise ou permet un tel acte. L'admission de l'article 17 de la loi sur le contrat de travail comme base légale suffisante pour prendre connaissance de communications électroniques effectuées par les employés est toutefois controversée[327].

En outre, rappelons que la C.C.T. nº 81 - à la supposer applicable à la surveillance des communications téléphoniques -, autorise l'employeur à prendre connaissance des communications de ses travailleurs, ne peut déroger à une interdiction légale d'interception et de prise de connaissance des communications électroniques. En effet, la C.C.T. nº 81 ne peut déroger à une interdiction posée par une loi[328]. Dès lors, l'employeur pourrait, selon nous, rencontrer certaines difficultés même s'il invoque la C.C.T. nº 81 comme base légale pour prendre connaissance d'informations transmises par voie de communication électronique.

3. L'enregistrement des communications commerciales et des communications téléphoniques dans le cadre des *call center*.

184. Comme évoqué ci-avant[329], l'article 128 de la loi du 13 juin 2005 crée deux dérogations à l'article 125 de la même loi ainsi qu'aux articles 314*bis* et 219*bis* du Code pénal.

La première dérogation concerne l'enregistrement et la prise de connaissance de communications électroniques dans le seul but de se ménager la preuve d'une transaction commerciale ou d'une autre communication professionnelle. La loi impose toutefois que les parties impliquées dans la communication soient informées de l'enregistrement, des objectifs précis de ce dernier et de la durée de stockage de l'enregistrement, et ce dès avant l'enregistrement. Par ailleurs, les données devront être effacées au plus tard à la fin de la période pendant laquelle la transaction peut être contestée en justice.

La seconde dérogation a trait à l'enregistrement de communications électroniques et des données de trafic dans le cadre d'un *call center* en vue de contrôler la qualité du service. Dans cette hypothèse, il est exigé que les personnes qui travaillent dans le *call center* soient informées au préalable de la possibilité de prise de connaissance et d'enregistrement, du but précis de cette opération et de la durée de conservation de la communication et des données enregistrées (qui ne peut excéder un mois).

---

327 P. Leduc, « Le contrôle des communications données et reçues par le travailleur », *Revue Ubiquité*, 2000/5, p. 48.

328 Sur cette question et sur la violation de l'article 22 de la Constitution, voy. *supra*, chapitre 2, section 2, B.

329 Voy. chapitre 2, section 3, B, 3.

L'article 128 de la loi du 13 juin 2005 prévoit que ces deux dérogations sont sans préjudice du respect du prescrit de la loi du 8 décembre 1992.

4. Les impératifs techniques, le contrôle du bon état du réseau et l'état de nécessité

185. L'article 125 de la loi du 13 juin 2005 prévoit également que les impératifs techniques puissent justifier une dérogation à l'interdiction de prise de connaissance et l'enregistrement des informations transmises par voie de communication électronique. En outre, certains auteurs citent expressément l'état de nécessité comme circonstances qui permettraient à l'employeur de transgresser l'interdiction de prise de connaissance mentionnée[330].

Même si on voit mal ces exceptions s'appliquer au cas précis du contrôle du téléphone, il n'est pas exclu que la commission par le travailleur d'une infraction d'une gravité extrême puisse justifier que l'employeur enfreigne les articles 124 de la loi du 13 juin 2005 ou 314*bis* du Code pénal en vue d'empêcher la réalisation de l'infraction par le travailleur.

b. Les modalités du contrôle

186. L'employeur devra se conformer aux principes évoqués ci-avant, à savoir les principes de transparence, de finalité, de proportionnalité pour réaliser le contrôle de l'usage du téléphone par ses travailleurs. Dans tous les cas, l'employeur devra informer les travailleurs des contrôles qui existent. En outre, la finalité devra être explicitement annoncée : contrôle des coûts de communication, protection des coûts de l'entreprise, sécurité des communications, gestion de l'entreprise,…

Par ailleurs, l'employeur devra opter pour les modalités de contrôle du téléphone qui engendrent le moins d'ingérence dans la vie privée des travailleurs au regard des finalités poursuivies. Ainsi par exemple, l'enregistrement du contenu des conversations téléphoniques ne sera pas justifié si la finalité poursuivie est la gestion des coûts de communication[331].

En termes de modalités de contrôles techniquement possibles, plusieurs cas de figure peuvent être envisagés : tantôt l'employeur voudra contrôler le

330 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 71; O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 52.

331 Voy. pour l'application de ces principes pour les services bancaires téléphoniques, la recommandation n° 1/2002 du 22 août 2002 de la Commission de la protection de la vie privée sur l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, www.privacycommission.be. Dans un même ordre d'idées, le recours à un dispositif « Zoller », par exemple, sera disproportionné pour surveiller l'activité d'un travailleur (F. Lagasse et M. Milde, « Protection de la personne et vie privée du travailleur. Investigation et contrôle sur les lieux du travail », *Orientations*, 1992, p. 153).

contenu des conversations téléphoniques (par l'écoute ou l'enregistrement des conversations téléphoniques), tantôt il voudra vérifier les données de communication (lesquelles peuvent être enregistrées et communiquées par l'opérateur sur la facture, ou stockées sur le central téléphonique de l'entreprise). La distinction entre le contrôle des données de communication et le contrôle du contenu des communications téléphoniques est d'ailleurs classique[332].

Nous analyserons ci-dessous en premier lieu le contrôle des conversations téléphoniques des travailleurs (écoute et enregistrement) (§ 1er), et ensuite celui des données relatives à l'utilisation du téléphone (§ 2).

§ 1er. L'enregistrement ou la prise de connaissance du contenu des communications

187. Dans certains cas, l'employeur pourra souhaiter prendre connaissance du contenu des conversations téléphoniques, ce qui passera le plus souvent par leur enregistrement.

L'application stricte des dispositions légales concernant l'interception ou la prise de connaissance de communications électroniques (articles 314*bis* du Code pénal et 124 de la loi du 13 juin 2005) empêche en principe l'enregistrement par un tiers de la conversation téléphonique sans le consentement de toutes les parties à la communication.

188. La Commission de la protection de la vie privée avait analysé la problématique dans le contexte spécifique du secteur bancaire et recommandé, dans un avis du 22 août 2002, d'obtenir le consentement libre et éclairé des personnes concernées, tant des clients que des employés[333]. La Commission recommandait que le consentement préalable des clients (ou autres parties à la conversation) soit obtenu de manière individuelle et porte sur des conditions d'utilisation suffisamment claires[334]. Concernant le consentement des employés, il devait également être obtenu de manière individuelle. Selon la Commission, une note de service ou une mention dans le règlement de travail ne pouvait être suffisant : il s'agissait de combiner le consentement individuel de l'employé avec la négociation d'un texte général auquel seraient associés les représentants des employés. Cependant, ce texte est antérieur à la loi du 13 juin

---

332 Voy. S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. du Jeune Barreau de Bruxelles, 2005, p. 174 ; P. LEDUC, « Le contrôle des communications données ou reçues par le travailleur », *R.D.T.I. – Ubiquité*, 2000, p. 41.

333 Commission de la protection de la vie privée, Recommandation 1/2002 relative à l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, 22 août 2002, www.privacycommission.be.

334 On peut considérer que l'annonce, préalable à la conversation, que la communication pourra être enregistrée, constitue une base suffisante pour justifier l'existence d'un consentement.

2005 et à son article 128 et nous semble dépassé, dès lors que des exceptions spécifiques à l'interdiction d'interception des communications électroniques sont désormais renseignées dans cette disposition.

À cet égard, il nous semble que si, comme nous l'avons vu, différentes dispositions créaient des exceptions à l'exigence de toutes les parties à la communication, seules celles dudit article 128 sont pertinentes dans le contexte de la prise de connaissance du contenu des communications téléphoniques.

La première de ces exceptions contenue à l'article 125, 1° de la loi du 13 juin 2005 requérait l'existence d'une disposition légale permettant ou autorisant une telle prise de connaissance. L'article 17 de la loi du 3 juillet 1978 invoqué comme fondement légal à l'exercice normal de l'autorité de l'employeur, ne nous paraît pas pouvoir justifier une telle ingérence dans la vie privée des travailleurs. Les nécessités techniques visées à l'article 125, 2° ne nous paraissent pas non plus pertinentes pour justifier l'écoute ou l'enregistrement de communications téléphoniques. Ne restent donc que les dérogations prévues à l'article 128 de la loi du 13 juin 2005 qui ont trait, d'une part à l'enregistrement de communications commerciales à des fins de preuve et, d'autre part, aux contrôles de qualité du service dans les *call center*.

189. En toute hypothèse, le traitement devra être légitime et en conformité avec la loi du 8 décembre 1992. Ainsi, il est certain que le règlement concernant d'utilisation du téléphone devra mentionner l'utilisation qui en sera permise et/ou tolérée, la possibilité d'un enregistrement de la conversation, et également la finalité poursuivie par l'employeur. Si la finalité poursuivie consiste seulement en la surveillance des prestations de ses employés, l'écoute téléphonique devra selon nous être considérée comme un moyen de contrôle disproportionné.

Notons qu'un arrêt rendu par la Cour du travail de Liège le 5 mai 1985 était allé dans un tout autre sens en justifiant le droit de contrôle par le fait que l'employeur est le propriétaire du réseau de communication « et que l'employeur peut utiliser son téléphone pour surveiller son personnel, surtout en cas de suspicion, ainsi que la technique moderne de la télévision pour surveiller ses vendeuses ou la boîte noire pour surveiller notamment la conscience professionnelle de son pilote »[335]. Le Tribunal de travail de Bruxelles a même pu considérer, que ce ne serait que lorsque l'usage à titre privé du téléphone aurait fait l'objet d'une autorisation préalable que le travailleur pourrait se retrancher derrière le principe du respect de la vie privée[336]. Cette jurisprudence est tou-

335 C. trav. Liège, 5 mai 1985, *J.T.T.*, 1985, p. 472.

336 Trib. trav. Bruxelles, 7 février 1990, *Pas.*, 1990, II, p. 88.

tefois antérieure à la loi du 21 mars 1991 et à l'arrêt *Niemietz*[337] et ne pourrait selon nous se justifier à l'heure actuelle[338].

190. Une autre question est de savoir si l'une des parties à une communication peut produire l'enregistrement de cette conversation. Dès lors que la partie qui produit un enregistrement n'est pas partie à la communication, les articles 124 de la loi du 13 juin 2005 et 314*bis* du Code pénal n'y font pas obstacle. Une telle production serait donc en principe recevable en justice.[339] La Cour de cassation a estimé que « celui qui tient une conversation téléphonique ne peut invoquer le droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance, mentionné aux articles précités, à l'égard de l'intervenant à cette conversation, faisant lui-même participer cet intervenant à l'objet de ce droit »[340]. La Cour a toutefois précisé que « le juge qui apprécie si l'usage est autorisé, est tenu d'inclure dans son jugement le critère de l'attente raisonnable du respect de la vie privée. Ce critère porte notamment sur le contenu et les circonstances dans lesquelles la conversation a eu lieu »[341].

§ 2. La prise de connaissances de données de communication

191. La question de savoir si un employeur peut utiliser les données relatives aux communications passées par les travailleurs au moyen des téléphones mis à leur disposition (GSM, ou téléphone fixe installé à la maison ou au bureau) est moins claire. En sa qualité d'abonné, l'employeur peut avoir accès aux données de facturation, celles-ci révélant notamment le nombre d'appels, leurs destinataires, les heures de ceux-ci, et leur durée. Nonobstant certains obstacles légaux sur lesquels nous reviendrons ci-dessous, on constate que plusieurs décisions ont admis la production de factures destinées à établir l'existence d'appels passés à des fins privées sur un téléphone de l'entreprise en considérant que l'employeur pouvait produire les listings d'appels fournis par son opérateur de téléphonie.

La loi du 13 juin 2005 relative aux communications électroniques établit la liste des droits des utilisateurs finals d'un service de téléphonie (tels les travailleurs) en les distinguant de l'abonné (tel un employeur).

---

337 C.E.D.H., *Niemietz c. Allemagne*, 16 déc. 1992, *Publ. Cour. eur. D.H.*, série A, n° 251-B.

338 S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. du Jeune Barreau de Bruxelles, 2005, p. 177 ; voy. également Trib. trav. Bruxelles, 26 mars 1990, *Chron. D.S.*, 1990, p. 154.

339 Voy. les références citées en ce sens à cet égard *in* : S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Éd. du Jeune Barreau de Bruxelles, Bruxelles, 2005, p. 177 ; voy. Cass., 9 janvier 2001, P990235N, www.juridat.be ; C. trav. Liège 23 mai 1984, *J.L.M.B.*, 1984, p. 82.

340 Cass., 9 janvier 2001, P990235N, www.juridat.be.

341 Cass., 9 septembre 2008, P.08.0276.N, www.juridat.be.

Ainsi l'article 122, § 2 de la loi du 13 juin 2005 prévoit-il que les opérateurs peuvent traiter les données trafic concernant les utilisateurs et les abonnés et qu'une information préalable doit leur être fournie quant à ce. L'article 110, § 1er et son arrêté d'exécution du 27 avril 2007 fixent le niveau de détail de la facture de base. Cet arrêté ne prévoit pas que les numéros d'appel doivent figurer sur cette facture. L'article 110, § 2 de la loi dispose cependant qu'en cas de contestation de la facture de base, les abonnés peuvent obtenir gratuitement, sur demande, une facture détaillée. L'exposé des motifs de la loi ne précise pas quelles données peuvent être ainsi obtenues et ne pose dès lors aucune limite. En outre, on relèvera que la loi prévoit par ailleurs que certains numéros appelés (tels certains numéros d'urgence) ne figureront jamais sur les factures. On peut en déduire qu'*a contrario*, rien ne s'oppose à ce qu'un employeur puisse se voir communiquer des numéros d'appel formés par ses travailleurs dans le cadre d'abonnements pris par l'employeur.

Dans le même sens, on notera que les travaux préparatoires de la loi du 30 juin 1994 qui a donné lieu à l'article 314*bis* du Code pénal envisagent la possibilité pour l'employeur de relever les numéros de téléphone appelés par ses travailleurs et excluent par conséquent les données téléphoniques de l'interdiction contenue dans l'article 314*bis*[342].

192. Si on se réfère en revanche aux principes 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, celle-ci ne prévoit un droit d'accès qu'à la personne concernée par les données. À notre sens, seul le travailleur peut exercer ce droit. L'application de l'article 124 de la loi du 13 avril 2005 induit également une telle solution dès lors que l'employeur, en tant que tiers à la communication, ne peut prendre connaissance de telles données sans le consentement de toutes les personnes concernées par celle-ci. En toute hypothèse, la prise de connaissance de telles données et l'utilisation dans le cadre d'un contrôle du travailleur s'inscrivent dans le cadre d'un traitement de données à caractère personnel au sens de la loi du 8 décembre 1992 qui doit, à ce titre, être réalisé dans le respect de toutes les conditions fixées par cette loi (en ce compris, par exemple, l'obligation d'information préalable du travailleur).

193. Nous n'avons cependant recensé aucune jurisprudence relative à ce problème dans le cadre de la nouvelle loi et qui se prononcerait sur le droit pour l'employeur d'accéder et/ou d'utiliser à des fins de contrôle aux données

---

342 S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies » *in* J.-Fr. LECLERCQ (dir.), *Vie privée du travailleur et prérogatives patronales*, Éd. du Jeune Barreau de Bruxelles, Bruxelles, 2005, p. 174.

d'appel de ses travailleurs en tenant compte de la coexistence de toutes ces dispositions.

Cependant, plusieurs décisions, antérieures à la loi du 13 juin 2005, avaient déjà accepté que l'employeur puisse avoir accès aux données d'utilisation du téléphone de ses travailleurs pour contrôler les activités de ses employés.

Ainsi, la Cour du travail de Gand a eu à connaître d'un cas de licenciement pour motif grave du fait que l'employé avait notamment tenu des conversations privées avec le matériel mis à sa disposition[343]. La Cour a considéré que la production et l'analyse des factures par l'employeur était un usage normal des factures, qui étaient adressés à l'employeur pour qu'il les paie. L'employé devait en effet savoir que ce type de contrôle pouvait avoir lieu. Notons que la Cour a également estimé qu'il ne pouvait être reproché à un cadre supérieur, non tenu par des limites horaires pour l'exécution de son travail, d'avoir des communications d'ordre privé.

Devant un cas d'espèce similaire, la Cour du travail de Liège a considéré que la production de factures de téléphones, démontrant qu'un numéro avait été appelé à plusieurs reprises par un employé sans être le numéro d'un client ou d'un fournisseur, était un mode de preuve admissible[344]. Par contre, en l'absence de règles précises au sein de l'entreprise relatives à l'utilisation du téléphone, et vu la tolérance existant en Belgique face à une utilisation privée vers des appels nationaux, la Cour a considéré que le motif grave n'était pas établi.

Dans une autre affaire, le Tribunal du travail de Bruxelles a considéré que l'employeur pouvait fonder son enquête sur des listings d'appels obtenus de l'opérateur mobile pour déterminer l'origine et l'heure des appels passés avec le GSM professionnel confié à son travailleur[345]. Selon le Tribunal, « le droit d'une entreprise à voir respecter son image de marque auprès de sa clientèle et des tiers implique qu'elle puisse s'opposer à ce que des membres de son personnel se connectent à des sites pornographiques pendant l'exécution de leur contrat de travail, avec les outils télématiques ou de téléphonie mobile dont elle est propriétaire et qu'elle leur confie pour l'exécution de leur travail ». Le Tribunal a estimé que le contrôle effectué par l'employeur n'était pas excessif dès lors qu'une interdiction d'utilisation du téléphone à des fins privées avait clairement été formulée, et que le contrôle des factures mensuelles avait eu lieu après un premier avertissement des travailleurs concernés (le dépistage n'était donc pas systématique). En outre, le travailleur avait été entendu avant son licenciement, ce qui rendait la procédure contradictoire.

---

343 C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2002, p. 41.

344 C. trav. Liège, 25 octobre 2001, *J.T.T.*, 2002, p. 40.

345 Trib. trav. Bruxelles (3e ch.), 16 septembre 2004, *J.T.T.*, 2005, p. 61.

On observe ici que le tribunal a apprécié la validité de la preuve en vertu des principes déjà exposés ci-avant, et notamment au regard de l'obligation de transparence (interdiction préalable d'un usage privé du téléphone, information quant aux contrôles,…) et au principe de proportionnalité (avertissement préalable, audition de l'intéressé, absence d'examen systématique des données).

194. On notera également que l'avertissement général avant de procéder à une analyse précise des factures de GSM, l'audition préalable du travailleur avant de le sanctionner et l'information précise sur l'utilisation des téléphones sont des obligations inscrites dans la C.C.T. nº 81, dont l'application au cas du contrôle des communications téléphoniques est discutable[346].

En effet, comme nous l'avons soulevé *supra* (chapitre 2, section 5, B, 4), la procédure prévue par la C.C.T. semble n'avoir été conçue que pour viser les e-mails et la navigation internet.

À supposer que tel soit pourtant le cas, on pourrait imaginer que, par application du principe de proportionnalité que la C.C.T. nº 81 met en œuvre, et par analogie avec la procédure prévue dans la C.C.T., le contrôle individuel des données détaillées de facturation ne soit effectué que lorsque une anomalie a été détectée, comme par exemple, une facture au montant inhabituel, ou un nombre d'appels internationaux plus élevé que la normale, donnant lieu à un premier avertissement. Le principe de proportionnalité sera alors respecté puisque la prise de connaissance du détail des appels ne se fera qu'après avoir constaté que l'examen des différents postes globaux de la facture ne suffit pas à faire cesser l'abus.

4. Le contrôle du poste de travail et des fichiers et données stockés sur l'ordinateur du travailleur

a. Principes

195. La question de savoir dans quelle mesure l'employeur peut contrôler l'utilisation des ordinateurs mis à disposition des travailleurs, indépendamment des e-mails ou de l'internet, peut se poser lorsque l'employeur voudra accéder au contenu de l'ordinateur du travailleur ou contrôler l'usage qu'il en fait, par exemple en utilisant des logiciels conçus à cet effet.

Nous avons déjà examiné la question de savoir si un employeur peut interdire toute utilisation non professionnelle des outils informatiques mis à disposition. La Cour du travail de Gand a considéré que « l'employeur a le droit, en vertu de la loi relative aux contrats de travail, d'instaurer unilatéralement des

346 Voy. *supra,* chapitre 2, section 5, B. L'application de la C.C.T nº 81 n'est pas examinée dans la décision précitée du Tribunal du travail de Bruxelles.

directives et obligations quant à l'informatique, sans consensus ou implications des travailleurs »[347].

En toute hypothèse, même dans le cas où seul un usage professionnel est autorisé par l'employeur, cela ne l'autorise pas forcément à prendre connaissance des informations stockées dans le terminal sans respecter certains principes.

196. Nous considérons, avec Olivier Rijckaert, que les données stockées sur un support magnétique par le travailleur sont susceptibles de bénéficier de la protection liée au droit au respect de la vie privée[348].

Deux questions persistent toutefois : peut-on considérer que les articles 314*bis* du Code pénal et 124 de la loi du 13 juin 2005 s'appliquent aux données de communication électroniques stockées sur un ordinateur ? En outre, ces données sont-elles visées par les articles 460 du Code pénal et 29 de la Constitution qui protègent le secret des correspondances ?

197. La réponse à la première question nous semble claire : dès lors que l'article 124 de la loi du 13 juin 2005 a une portée plus large que celle de l'article 314*bis* du Code pénal qui limite sa protection à la durée de transmission de la communication, les communications stockées sur le disque dur de l'employé restent protégées par le secret des communications électroniques[349]. C'est dans ce sens que s'est par exemple prononcé la Cour du travail d'Anvers, qui reprochait à l'employeur de ne pas avoir obtenu le consentement du travailleur pour consulter le contenu des messages reçus[350]. Nous n'examinerons plus cette hypothèse dans le cadre de la présente section et renvoyons à la section qui est consacrée au contrôle des e-mails[351]. Par contre, les autres données, qui ne sont pas des données de communication électroniques, telles que les fichiers et dossiers, ne seront pas protégées par les dispositions de la loi du 13 juin 2005.

198. Quant à savoir si les données stockées sont protégées par le secret des correspondances, la réponse devrait être nuancée. Ainsi, certains considèrent que, vu la portée restrictive des articles 29 de la Constitution et 460 du Code pénal, les données stockées ne devraient pas être considérés comme de la correspondance au sens de ces dispositions[352]. Cependant, le Tribunal du travail de

---

347 C. trav. Gand, 4 avril 2001, *J.T.T.*, 2002, pp. 49-52.

348 O. RIJCKAERT, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, pp. 45-46.

349 Voy. développement à ce sujet *supra* chapitre 2, section 3.

350 C. trav. Anvers, 1er octobre 2003, *J.T.T.*, 2004, p. 510.

351 *Cf.* n° 144 et suiv., *supra*.

352 O. RIJCKAERT, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, pp. 53-54 ; voy. également C. trav. Liège, 25 avril 2002, www.cass.be ; C. trav.

Verviers a estimé que le fait pour l'employeur de consulter les lettres privées, stockées sur l'ordinateur de travail, à l'insu de son employée, constituait une violation de l'article 29 de la Constitution et de l'article 8 de la C.E.D.H.[353].

Quoi qu'il en soit, il nous semble que les données stockées sur le support fixe de l'employé restent dans tous les cas protégées par les articles 8 de la C.E.D.H. et 22 de la Constitution. Dès lors, les principes de transparence, de proportionnalité, de légalité et de finalité devront être respectés par l'employeur effectuant un contrôle des données stockées par l'employé, que celles-ci soient ou non professionnelles.

199. Il en sera de même, selon nous, concernant le contrôle de l'usage des postes de travail des travailleurs. À cet égard, mentionnons l'arrêté royal relatif au travail des équipements à écran de visualisation du 27 août 1993[354], disposant que, concernant l'interface ordinateur/homme, « aucun dispositif de contrôle quantitatif ou qualitatif ne peut être utilisé l'insu des travailleurs ». On pense par exemple à certains logiciels qui rapportent en temps réel à l'employeur les activités des personnes situées derrières leur poste de travail.

L'utilisation de ce genre de procédés devra non seulement répondre au prescrit de l'arrêté royal susmentionné, mais également à la loi du 8 décembre 1992, dès lors qu'un traitement de données est réalisé, et aux articles 8 de la C.E.D.H. et 22 de la Constitution qui protège la vie privée des individus. On peut d'ailleurs se demander si l'installation d'un dispositif permanent de contrôle des outils informatiques ne se heurte pas au principe de proportionnalité consacré par ces deux dernières dispositions.

b. Distinction entre données professionnelles et données privées

200. Il nous semble que la distinction opérée par O. Rijckaert entre données et documents à caractère privé et personnel, d'une part, et données et documents à caractère professionnel, d'autre part, pour fonder une différence de traitement quant à l'appréciation du contrôle posé, est pertinente pour apprécier l'ingérence de l'employeur dans la vie privée de son travailleur. En ce qui concerne les documents à caractère professionnel, ils ne se distingueraient en réalité pas fondamentalement de documents traditionnels sur papier[355].

Liège, 23 mars 2004, www.cass.be.

353 Trib. trav. Verviers, 20 mars 2002, *J.T.T.*, 2002, p. 183.

354 A.R. du 27 août 1993 relatif au travail des équipements à écran de visualisation, *M.B.*, 7 septembre 1993, p. 19579.

355 O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 54.

Selon l'auteur, les principes de finalité, de transparence, et de proportionnalité devraient être appréciés plus souplement que lorsqu'il s'agit de contrôler des documents privés. Reste à savoir, évidemment, comment déterminer si un document ou une donnée peut être considéré comme privé. Selon O. Rijckaert, le travailleur devrait spécifiquement identifier le dossier ou le fichier concerné comme privé[356].

C'est en ce sens que la jurisprudence française a tranché la question. Ainsi, l'arrêt *Nikon* rendu par la Cour de cassation française avait affirmé 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»[357]. Depuis lors, la Cour de cassation française a eu l'occasion de baliser cette jurisprudence en précisant dans un arrêt du 17 mai 2005[358], que la prise de connaissance des fichiers contenus sur le disque dur de l'ordinateur mis à sa disposition identifiés comme personnels par l'employé ne pouvait avoir lieu qu'en présence de ce dernier ou celui-ci dûment appelé. La Cour suprême française a ensuite affirmé dans deux arrêts de 2006[359], l'existence d'une présomption du caractère professionnel des fichiers enregistrés sur le disque dur de l'ordinateur du salarié. Ainsi, dans un arrêt du 30 mai 2007[360], elle a estimé que le juge ne pouvait se contenter de constater que le contenu d'e-mails consultés par l'employeur revêtait un caractère privé mais qu'il aurait dû vérifier si les fichiers ouverts sur le matériel mis à la disposition par l'employeur, avaient été identifiés comme étant personnels par le salarié.

201. Cependant, on ajoutera que les solutions retenues par la jurisprudence française ne sont selon nous pas transposables en Belgique, dès lors que la jurisprudence belge n'a pas consacré de principe de présomption de caractère professionnel des données stockées sur un ordinateur.

On relève toutefois que, dans un arrêt du 11 janvier 2007[361], la Cour du travail de Liège a considéré que la production d'un document revêtant manifestement un caractère personnel (il s'agissait d'un tableau détaillant les charges du ménage d'une employée) enregistré sur le disque dur de l'ordinateur mis

356 O. Rijckaert, «Surveillance des travailleurs: nouveaux procédés, multiples contraintes», *Orientations*, n° spécial 35 ans, mars 2005, p. 54.

357 Cass. Fr., 2 octobre 2001, Arrêt n° 4164, www.droit-technologie.org.

358 Cass. Fr., 17 mai 2005, Pourvoi n^{os} 03-40.017, www.legifrance.gouv.fr.

359 Cass. Fr., 18 octobre 2006, Pourvoi n^{os} 04-48025, www.legifrance.gouv.fr; Cass. Fr., 18 octobre 2006, Pourvoi n^{os} 04-47400, www.legifrance.gouv.fr.

360 Cass. Fr., 30 mai 2007, Pourvoi n^{os} 05-43102, http://www.droit-technologie.org.

361 C. trav. Liège, section de Namur, 11 janvier 2007, *R.R.D.*, 2007, p. 488, note K. Rosier et S. Gilson.

à la disposition de la travailleuse par son employeur ne viole pas le droit au respect de la vie privée dans la mesure où il ne s'agit pas d'un courrier privé.

Elle estime qu'en enregistrant un document à caractère privé sur un ordinateur de l'entreprise, la travailleuse a pris le risque que toute personne ayant accès à cet ordinateur en prenne connaissance. Par contre, la Cour ne se penche pas sur la question de savoir si le document était d'une manière ou d'une autre identifié de par sa classification dans les fichiers ou de par sa dénomination comme revêtant un caractère privé.

202. Le critère retenu dans l'arrêt de la Cour du travail de Liège pour délimiter la protection nous paraît problématique au regard du droit au respect de la protection de la vie privée. En effet, la protection de la vie privée au travail consacrée notamment par l'arrêt *Niemietz* de la C.E.D.H. ne se limite pas à la correspondance[362]. Ainsi, selon nous, l'article 8 de la C.E.D.H. et l'article 22 de la Constitution belge imposent que l'on ne puisse en principe pas, à l'insu du travailleur, prendre connaissance de documents à caractère privé stockés sur l'ordinateur qui lui est attribué[363].

Le fait que le travailleur puisse concevoir que techniquement toute personne qui se servirait de l'ordinateur pourrait prendre connaissance du document nous semble être un critère insatisfaisant pour exclure la protection de la vie privée. Si une ingérence est possible dans la vie privée du travailleur, celle-ci doit satisfaire aux critères de légalité, de finalité et de proportionnalité. En particulier, le critère de légalité commande que la personne concernée ait été informée de la possibilité d'un tel acte[364], d'où l'intérêt de le prévoir dans une réglementation de l'utilisation de l'outil informatique[365].

203. Concernant une affaire, relativement ancienne, où un travailleur avait été licencié pour avoir accédé à l'ordinateur d'un autre employé sans autorisation, la Cour du travail de Gand a jugé que le droit au respect de la vie privée garanti par la C.E.D.H. et la loi du 8 décembre 1992 ne sont pas violés lorsqu'on

---

362 Voy. Notamment Cour eur. D.H., *Niemietz c. Allemagne*, arrêt du 16 déc. 1992, *Publ. Cour. eur. D.H.*, série A, n° 251-B ; Cour eur. D.H., *Halford c. Royaume-Uni*, arrêt du 25 juin 1997, http://www.echr.coe.int ; Cour eur. D.H., *Copland c. Royaume-Uni*, arrêt du 23 avril 2007, http://www.echr.coe.int/echr/.

363 Cass. Fr., 17 mai 2005, n^{os} 03-40.017, www.legalis.net ; Cass. Fr., 2 octobre 2001, arrêt n° 4164, www.legalis.net (dit arrêt *Nikon*) ; Trib. trav. Hasselt, 21 octobre 2002, *Chron. D.S.*, 2003, p. 197.

364 F. Hendrickx, « Privacy en arbeidsrecht », *Jura Falconis*, 1998-99, n° 4, pp. 625-626 ; Th. Claeys et D. Dejonghe, « Gebruik van *e-mail* en internet op de werkplaats en contrôle door de werkgever », *J.T.T.*, 2001, p. 122 ; O. Rijckaert, « Surveillance des travailleurs : nouveaux procédés, de multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 54 ; J.-Fr. Neven, « Les principes généraux : les dispositions internationales et constitutionnelles », *in* J.-Fr. Leclerq (dir.), *Vie privée du travailleur et prérogatives patronales*, Bruxelles, Éd. Jeune Barreau de Bruxelles, pp. 24 et 25.

365 Rappelons toutefois que la consultation des e-mails envoyés ou reçus est soumise en droit belge à une législation particulière.

contrôle la réalité d'actes supposés accomplis dans le but de s'introduire dans la messagerie électronique d'un autre employé[366]. La Cour considère également que la surveillance, à l'intérieur d'une entreprise, de l'utilisation du réseau mis à disposition ne tombe pas sous le coup de l'article 314*bis* du Code pénal. L'employeur était donc fondé à produire les *log files* de l'ordinateur consulté pour établir la réalité de l'intrusion dans l'ordinateur et ce faisant, ne violait pas la vie privée du travailleur ni l'article 314*bis* en question.

La Cour précise en outre qu'il est préférable que de tels contrôles soient contradictoires pour faciliter la preuve des faits. Cette question est intéressante dès lors que, même si la preuve pourra être considérée comme admissible devant un tribunal, il faudra encore que l'employeur qui voudrait s'en prévaloir garantisse qu'elle ne puisse être contestée en justice par l'employé. En effet, une trace informatique peut facilement être modifiée, et sa fiabilité pourra être aisément contestée. Dans ce cas, l'appel à un huissier pourrait être une solution opportune afin de préserver la valeur probante de preuve.

204. À cet égard, le Tribunal du travail de Hasselt a dû se prononcer sur la validité d'une preuve obtenue par l'examen du poste de travail d'un employé sans son autorisation, en présence d'un huissier de justice[367]. Le tribunal a néanmoins refusé la preuve au motif que les principes de proportionnalité et de transparence n'avaient pas été respectés. L'examen du contenu de l'ordinateur était en effet, selon le tribunal, disproportionné. Ce n'est donc pas ici la valeur probante des constats d'huissier qui a été contestée, mais bien la licéité de la preuve apportée eu égard au principe de respect de la vie privée.

À l'opposé, un arrêt de la Cour du travail de Bruxelles a rejeté des preuves informatiques relatives à des agissements d'un employé, non pas au motif que celles-ci étaient contraires aux dispositions protégeant la vie privée, mais en raison du fait qu'il est possible en théorie de manipuler les données collectées pour en faire une preuve[368].

Notons qu'en France, la possibilité de demander l'autorisation à un juge de saisir le matériel informatique en cas de suspicion de fraude par un employé a été consacrée par la Cour de cassation, qui considère que cette possibilité ne peut être tenue en échec par les dispositions protectrices de la vie privée[369].

205. Devant l'incertitude du statut de la protection des données de l'ordinateur d'un travailleur, il nous semble que l'employeur devra aller au maximum des obligations imposées par l'article 8 C.E.D.H., et notamment informer

366 C. trav. Gand, 4 avril 2001, *J.T.T.*, 2002, p. 49.

367 Trib. trav. Hasselt, 21 octobre 2002, *Chron. Dr. Soc.*, 2003, p. 197.

368 C. trav. Bruxelles, 7 mars 2003, A.R., n° 42718, www.cass.be.

369 Cass. Fr., Ch. soc., 23 mai 2007, arrêt n° 1146, www.courdecassation.fr.

les travailleurs des usages permis et interdits de l'ordinateur (cryptage, usage du mot de passe, règles de délégation, etc.) tout en se gardant d'effectuer des contrôles sur le poste de travail de l'employé qui ne seraient en rien justifiés par les circonstances, sous peine de voir le contrôle disproportionné eu égard à la finalité poursuivie et aux indices de suspicion de faute de la part du travailleur. En tout état de cause, il semble préférable de procéder à un examen contradictoire du contenu du poste informatique, en présence du travailleur, afin de se prémunir des contestations ultérieures de ce dernier.

206. On notera également que se posera souvent la problématique de l'accès à un ordinateur d'un travailleur en son absence, lorsque cet accès est nécessaire à la continuité du travail en entreprise. Dans ce dernier cas, on peut ne peut que conseiller d'obtenir l'autorisation d'accès par l'employé à son poste de travail, et à tout le moins, de l'informer (par exemple par le biais de circulaires internes) de la politique d'accès aux postes de travail en cas d'absence (congé, maladie) des travailleurs. Rappelons qu'il a déjà été considéré que l'accord du travailleur absent quant à l'utilisation de son poste de travail peut être implicite[370].

D. Les informations obligatoires

207. Rappelons que, quel que soit le traitement de données à caractère personnel concerné, l'article 9 de la loi du 8 décembre 1992 prévoit que les responsables de traitement doivent informer les personnes concernées de plusieurs éléments. Ainsi, en vertu de cette disposition, le travailleur devra au moins être informé, lorsque les données auront été directement obtenues auprès du travailleur, sur les aspects suivants du traitement[371] :

- le nom et l'adresse du responsable du traitement et, le cas échéant, de son représentant ;
- des finalités du traitement ;
- l'existence du droit de s'opposer, sur demande et gratuitement, aux traitements de marketing direct (ce qui sera, on peut l'imaginer, rarement le cas dans le cadre d'une relation de travail) ;
- d'autres informations supplémentaires, notamment :
  - les destinataires ou les catégories de destinataires des données,
  - le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse,
  - l'existence d'un droit d'accès et de rectification des données la concernant.

---

370 Voy. à cet égard l'arrêt de la Cour du travail d'Anvers déjà cité : C. trav. Anvers, 8 janvier 2003, R.G. n° 2020255, www.cass.be.

371 B. Docquir, *Le droit à la vie privée*, Bruxelles, Larcier, 2008, pp. 187-191.

208. En outre, lorsque les données ne sont pas obtenues directement auprès de la personne concernée, il conviendra d'informer cette dernière des catégories de données concernées.

Alors que les premières informations constituent le minimum des informations à communiquer, les informations supplémentaires seront fournies sauf dans la mesure où, compte tenu des circonstances particulières dans lesquelles les données sont obtenues, elles ne sont pas nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données[372].

Aussi, outre ces informations, qui constituent le socle minimum d'informations à communiquer[373], l'employeur s'efforcera-t-il de fournir les informations nécessaires pour assurer à l'égard de la personne concernée un traitement loyal des données. À cet égard, il peut être utile de se référer aux informations que la Commission de la protection de la vie privée recommande de communiquer aux travailleurs dans le cas du contrôle des e-mails et de l'usage de l'internet des travailleurs[374], ainsi que les recommandations du Groupe de l'Article 29 sur le même sujet[375].

Aucune autre information obligatoire n'est imposée pour instaurer un contrôle sur les outils de communication électronique des travailleurs, sauf en ce qui concerne les données de localisation par un opérateur, dont le traitement doit faire l'objet d'une information préalable auprès des utilisateurs. Ainsi, l'opérateur doit les informer des types de données de localisation traités, des objectifs précis du traitement, de la durée du traitement, des tiers éventuels auxquels ces données seront transmises, et de la possibilité de retirer à tout moment, définitivement ou temporairement, le consentement donné pour le traitement.

209. En sus des informations données en vertu de l'application de l'article 9 de la loi du 8 décembre 1992 et, le cas échéant, de l'article 123 de la loi du 13 juin 2005, nous avons vu que la C.C.T. nº 81, dans les cas où elle est appelée à s'appliquer, impose d'informer les travailleurs sur :

– la politique de contrôle ainsi que les prérogatives de l'employeur et du personnel de surveillance ;

---

372 T. Léonard et Y. Poullet, « La protection des données à caractère personnel en pleine (r)évolution. La loi du 11 décembre 1998 transposant la Directive 95/46/CE du 24 octobre 1995 », *J.T.*, 1999, pp. 388-389, nº 43 ; B. Docquir, *Le droit à la vie privée*, Bruxelles, Larcier, 2008, p. 189, nº 429.

373 Voy. le terme « au moins les informations énumérées ci-dessous » utilisé dans l'article 9 de la loi du 8 décembre 1992.

374 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

375 Document de travail du Groupe de l'Article 29 concernant la surveillance des communications électroniques sur le lieu de travail, 5401/01/FR/Final WP 55, adopté le 29 mai 2002, disponible à l'adresse http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf, pt. 3.1.3.1.

– la ou les finalités poursuivies ;
– le fait que des données personnelles soient ou non conservées, le lieu et la durée de conservation ;
– le caractère permanent ou non du contrôle ;
– 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 ;
– les droits, devoirs, obligations des travailleurs et les interdictions éventuelles prévues dans l'utilisation des moyens de communication électronique en réseau de l'entreprise ;
– les sanctions prévues au règlement de travail en cas de manquement.

Ces informations doivent être communiquées de manière collective ; les trois dernières informations doivent être communiquées individuellement[376].

210. On constate en tout cas que ces différents textes obligent l'employeur à communiquer une information portant aussi bien sur l'utilisation des moyens de communication (droits, devoirs, obligations et interdiction) que sur le contrôle de ceux-ci (surveillance, prérogatives, sanctions).

Ajoutons enfin que la loi instituant le règlement de travail du 8 avril 1965 impose de mentionner dans le règlement de travail les modes de mesurage et de contrôle du travail en vue de déterminer la rémunération[377], les droits et obligations du personnel de surveillance[378], et les pénalités, le montant et la destination des manquements qu'elles sanctionnent[379].

211. La C.C.T. nº 81 ne concerne que le secteur privé. Néanmoins, malgré ces règles très strictes, on constatera que la Commission de la protection de la vie privée a, dans un avis nº 10/2000 du 3 avril 2000, tenté de dégager des principes du point de vue de la protection des données à caractère personnel qui doivent présider au contrôle effectué par l'employeur[380]. Sur cette base notamment, le secteur public a développé des codes de conduite qui non seulement définissent les règles d'utilisation des outils mis à la disposition des travailleurs mais qui, en outre, précisent les mesures de contrôles qui peuvent être

376 *Cf.* chapitre 2, section 5, B.
377 Art. 6, 2°, de la loi du 8 avril 1965.
378 Art. 6, 5° de la loi du 8 avril 1965, lequel recoupe les termes de la C.C.T nº 81.
379 Art. 6, 6° de la loi du 8 avril 1965. L'article 16 de la loi rappelle que seules les sanctions prévues dans le règlement de travail pourront être appliquées.
380 Commission de la protection de la vie privée, Avis 10/2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, 3 avril 2000, www.privacycommission.be.

mises en œuvre[381]. Nous renvoyons à cet égard à la contribution de D. De Roy consacrée à cette question dans cadre du présent ouvrage.

E. La concertation sociale

212. L'établissement d'un document règlementant l'utilisation des outils informatiques, de quelque nature qu'il soit (contrat de travail, règlement de travail, note interne, etc.), devra idéalement faire l'objet d'une consultation avec les travailleurs ou leur représentants[382].

En effet, comme le rappelle le Conseil de l'Europe dans sa recommandation R (89) du 18 janvier 1989 précité, l'information et la consultation préalable des travailleurs sont capitales avant l'introduction de toute mesure susceptible d'atteindre la vie privée des travailleurs :

> « 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. »

---

381 Voyez le code de déontologie concernant l'utilisation des moyens informatiques et le traitement électronique de données au sein du SPF Économie, PME, Classes moyennes et Énergie, analysé par la Commission de la protection de la vie privée dans son avis nº 21 du 12 juillet 2006. Voy. également l'arrêté du Gouvernement de la Communauté française portant le code de bonne conduite des utilisateurs des systèmes informatiques, du courrier électronique et d'internet au sein des services du Gouvernement de la Communauté française et des organismes d'intérêt public relevant du comité de secteur XVII analysé par l'avis de la Commission de la protection de la vie privée nº 18/2005 du 9 novembre 2005 ; voy. encore le Code de bonne conduite à l'intention des membres du personnel du ministère de la Communauté flamande analysé par la Commission de la protection de la vie privée dans son avis du 18 décembre 2003.

382 Voy. par exemple les modes de concertations envisagés dans la section 3 de la loi du 8 avril 1965 instituant les règlements de travail.

213. Il conviendra, le cas échéant, de respecter la procédure de consultation prévue par la C.C.T. nº 39 lors de l'introduction d'une nouvelle technologie dans l'entreprise (*cf. supra,* chapitre 2, section 5, A).

Rappelons également l'existence de la loi du 20 septembre 1948 portant organisation de l'économie[383] et de la convention collective de travail nº 9 du 9 mars 1972[384]. En vertu de ces textes, le conseil d'entreprise doit être informé et consulté préalablement sur tout projet et mesures susceptibles de modifier la politique du personnel, l'organisation du travail ou les circonstances et les conditions dans lesquelles s'exécute le travail dans l'entreprise ou dans l'une de ses divisions. L'introduction d'une nouvelle technologie, modifiant l'organisation du travail ou les conditions d'exécution du travail constitue une hypothèse plausible, et il conviendra dans ce cas de tenir compte de ces textes et de procéder à une consultation du conseil d'entreprise[385].

214. La consultation sociale sera également parfois nécessaire pour compléter le consentement individuel du travailleur lorsque celui-ci est requis. Selon le Groupe de l'Article 29, la légitimité des opérations de traitement ne doit pas reposer exclusivement sur le consentement du travailleur. Un avis du Groupe de l'Article 29 rappelle que l'implication de toutes les parties prenantes par le biais de conventions collectives pourrait ainsi, selon le Groupe de l'Article 29, constituer une façon adéquate de réglementer l'obtention des déclarations de consentement dans de telles situations[386].

C'est dans ce sens qu'allait la proposition de loi concernant la géolocalisation analysée par la Commission de la protection de la vie privée[387] : selon le texte examiné, le traitement de données à caractère personnel ne pouvait être effectué qu'après accord des commissions paritaires *ad hoc*, du comité commun à l'ensemble des services publics ou des organes compétents en vertu du régime des relations collectives de travail, en d'autres termes, moyennant l'accord des syndicats.

---

383 *M.B.*, 27-28 septembre 1948.

384 Rendu obligatoire par A.R. du 12 septembre 1972 (*M.B.*, 8 février 1984).

385 Voy. Th. Claeys, N. Toussaint et D. Dejonghe, « L'utilisation des nouvelles technologies et de l'*e-mail* durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail », *in Le Contrat de travail et la nouvelle économie*, Bruxelles, Éd. Jeune Barreau de Bruxelles, 2001, p. 288.

386 Groupe de l'Article 29, Avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy, p. 11.

387 Proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, ayant fait l'objet d'un avis de la Commission de la protection de la vie privée nº 12/2005 du 7 septembre 2005, nº 16.

Par conséquent, lorsque le consentement individuel du travailleur est requis, la validité de ce dernier pourra être confortée par une concertation sociale préalable.

F. Le choix de l'instrument précisant les modalités des règles d'utilisation et du contrôle et permettant de recueillir le consentement du travailleur

215. Une fois que les règles d'utilisation et de contrôle des outils de communication électronique seront arrêtées, il conviendra de choisir le support adéquat pour le communiquer. L'information pourra se faire par voie d'annexe au contrat de travail, via le règlement de travail, par une convention collective d'entreprise, par information au conseil d'entreprise, instructions, règlements,… La C.C.T. cite d'ailleurs une série de documents pouvant contenir constituer les supports de cette information[388].

Le consentement du travailleur à la politique d'utilisation et/ou de contrôle n'est en principe pas requis[389]. Toutefois, le consentement du travailleur à certains contrôles pourra dans certains cas être nécessaire, notamment en cas de prise de connaissance de communications électroniques, ou lorsque cela s'avère une condition pour assurer la légitimité du traitement au regard de la loi du 8 décembre 1992. Il conviendra d'en tenir compte pour déterminer le support adéquat à la communication de ces modalités de contrôle.

Enfin, certaines modalités d'information et de consultation sociale par l'employeur devront également être respectées le cas échéant, pour adopter le document décrivant la politique de l'entreprise concernant l'utilisation des technologies et leur contrôle.

1. Le document dans lequel mentionner le règlement d'utilisation des outils informatiques

a. Contrat de travail

216. On peut envisager que le règlement d'utilisation des outils informatiques soit annexé au contrat de travail et fasse l'objet d'une acceptation individuelle par le travailleur, soit que cela soit stipulé dans le contrat, soit que document annexé soit signé pour acceptation.

Le contrat de travail - qui a une valeur supérieure au règlement de travail dans la hiérarchie des sources - ou une annexe à celui-ci, pourra dans

388 Voir commentaire de l'article 8 de la C.C.T. nº 81.

389 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 43.

tous les cas constituer un instrument valable pour informer les travailleurs des restrictions à l'usage des outils informatiques et des contrôles mis en place. L'inconvénient de cet outil est bien sûr le manque de souplesse pour adapter le document par la suite[390].

b. Règlement de travail

217. Le règlement de travail peut également contenir des informations relatives aux contrôles et aux usages d'application concernant l'utilisation des outils informatiques[391]. La loi du 8 avril 1965 instituant les règlements de travail impose d'ailleurs de mentionner dans le règlement de travail les modes de mesurage et de contrôle du travail en vue de déterminer la rémunération[392], les droits et obligations du personnel de surveillance[393] et les pénalités, le montant et la destination des manquements qu'elles sanctionnent[394].

Le règlement de travail sera donc le plus souvent le document juridique incontournable qu'il conviendra de modifier pour y intégrer ces éléments.

Pour rappel, l'établissement et la modification du règlement de travail devront passer par les mécanismes de consultation sociale que la loi instituant les règlements de travail impose[395].

On peut imaginer que le règlement d'utilisation des outils de communication électronique soit incorporé au règlement de travail. Rappelons toutefois que l'information des travailleurs doit se faire conformément au prescrit de la C.C.T. nº 81 et doit être aussi bien individuelle que collective.

c. Convention collective

218. L'option d'une convention collective, adoptée au niveau d'un secteur ou d'une entreprise, peut également être une solution pour permettre de reproduire la politique d'usage et de contrôle prédéfinie.

---

390 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 35.

391 Pour plus de développement à cet égard, voy. F. Hendrickx, *Privacy en arbeidsrecht,* Bruges, Die Keure, 1999, p. 69.

392 Art. 6, 2 ° de la loi.

393 Art. 6, 5° de la loi, lequel recoupe les termes de la C.C.T nº 81.

394 Art. 6, 6° de la loi. L'article 16 rappelle que seules les sanctions prévues dans le règlement de travail pourront être appliquées.

395 Consultation du conseil d'entreprise et, à défaut, des travailleurs, conformément aux articles 12 et 13 de la loi.

Toutefois, l'adoption d'un tel document est souvent lourde et devra englober un ensemble de pratiques pas toujours uniformes dans les différentes entreprises ou branches d'entreprises concernées[396].

d. Directives, notes internes et pratiques

219. Le recours à des notes internes et à des directives peut également s'envisager comme un moyen pour l'employeur de déterminer et de communiquer aux travailleurs les différentes modalités qui s'attachent à l'utilisation et au contrôle des outils de communication électronique. Le commentaire de l'article 8 de la C.C.T. nº 81 mentionne d'ailleurs explicitement cette voie d'information comme une manière de communiquer les informations obligatoires.

Celles-ci peuvent être données par voie de directive ou de note interne signée par chaque travailleur pour réception, d'affichage sur l'ordinateur du travailleur à chaque connexion, par e-mail interne, ou encore par voie d'affichage. On peut même imaginer que cette information soit relayée en interne par des formations pour expliquer et/ou préciser comment les directives communiquées devront être appliquées concrètement[397].

220. En ce sens, notons que l'usage est évoqué par l'article 51, 9° de la loi du 5 décembre 1968 sur les conventions collectives de travail et les conventions paritaires comme source d'obligations dans les relations de travail. À cet égard, la Cour européenne des droits de l'homme a déjà pu considérer que des pratiques bien établies et connues des intéressés pouvaient justifier une immixtion dans la correspondance et la vie privée des individus, eu égard notamment à la prévisibilité de cette pratique[398]. L'analyse de la Cour doit cependant être nuancée et ne pourra être admise que dans certaines circonstances bien précises, la Cour rappelant au passage que de telles pratiques ne peuvent toutefois jamais déroger aux dispositions impératives de la loi et qu'en outre, leur accessibilité et prévisibilité doivent rencontrer les standards de légalité applicables en la matière. On notera également que le simple usage présente les inconvénients d'un manque de stabilité et de la question de la preuve de celui-ci.

Les plus grandes précautions devront donc être prises lorsqu'il s'agira d'admettre que des pratiques peuvent justifier un contrôle de la part de l'employeur[399]. Il nous semble évident que des documents écrits répondent mieux à la condition d'accessibilité et de prévisibilité et doivent être préférés à des

---

396 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 35.

397 A. Peiffer, A. Matthijs et E. Verlinden, *Privacy in de arbeidrelatie – Gids voor het voeren van een privacybeleid*, Gent, Story, 2008, p. 40.

398 C.E.D.H., arrêt *Silver*, 25 mars 1995, *Rec.*, Série A., vol. 61, § 88.

399 F. Hendrickx, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 71.

pratiques floues et susceptibles de plusieurs interprétations. Quoi qu'il en soit, le prescrit de la C.C.T. nº 81 se contentera difficilement de l'existence de simples pratiques pour satisfaire à l'obligation d'information qu'elle édicte[400]. En effet, un ensemble d'informations doivent être communiquées, à la fois de manière individuelle et collective. Il sera difficile de considérer que l'on rencontre cette obligation par la seule constatation d'une pratique établie au sein de l'entreprise[401].

2. Le document dans lequel recueillir le consentement du travailleur

Dans certains cas, l'information du travailleur ne sera pas suffisante et il conviendra de recueillir son consentement. Rappelons que l'implication de toutes les parties prenantes par le biais de conventions collectives pourrait ainsi constituer une façon adéquate de réglementer l'obtention des déclarations de consentement dans de telles situations[402], dès lors que le consentement doit être libre et spécifique, caractéristiques difficiles à garantir dans le cadre d'une relation de subordination.

a. Contrat de travail

221. On peut imaginer que le travailleur donne son consentement dans le contrat de travail au contrôle de certaines activités générées par les moyens informatiques mis à sa disposition.

Toutefois, rappelons que pour garantir que le caractère libre du consentement du travailleur sera considéré, il est préconisé de le doubler d'une concertation sociale ayant abouti à un accord sur le contrôle en question.

Dès lors, dans ces conditions, l'accord d'un travailleur donné sur un document comme le contrat de travail offre selon nous les garanties recommandées par le Groupe de l'Article 29 et de la Commission de la protection

---

400 Voy. art. 7, 8 et 9 de la C.C.T. nº 81.

401 Les employeurs soulèvent très souvent l'argument selon lequel les travailleurs auraient dû savoir que tel usage était interdit ou que tel contrôle était mis en place. Or, la preuve d'une telle connaissance devra idéalement être rapportée par écrit pour ne pas laisser place à une quelconque marge d'interprétation de pratiques par définition mouvantes, non définies et difficiles à constater. Ainsi, l'accès à la boîte e-mail d'un travailleur pendant son absence, même s'il constitue une pratique courante en entreprise, devra idéalement être confirmé dans un document au lieu d'être considéré comme un droit acquis de l'employeur à défaut de contestation de l'employé.

402 Groupe de l'Article 29, Avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy; Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be.

de la vie privée quant au caractère libre de ce consentement si un tel consentement vient conforter une concertation sociale préalable. Il pourrait toutefois être objecté que ce consentement anticipatif n'est pas suffisamment spécifique.

b. Règlement de travail

222. Une des faiblesses du règlement de travail est qu'il ne pourra en principe pas tenir lieu de consentement, dès lors, que celui-ci doit être individuel et spécifique. Il ne sera par conséquent pas possible de considérer qu'un règlement de travail, même négocié au sein de l'entreprise, sera assimilé à un consentement individuel tel qu'il est requis, le cas échéant.

c. Convention collective

223. La valeur d'une renonciation à un droit fondamental (celui à la protection de sa vie privée) par le biais d'un accord collectif est discutable[403]. Rappelons à cet égard que la loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions paritaires empêche de déroger aux normes impératives[404]. Un test constitutionnel des dispositions de la convention collective limitant le droit à la vie privée des travailleurs devrait donc être possible sur cette base[405].

224. Tout comme pour le règlement de travail, se pose en effet la question de déterminer la valeur d'un consentement collectif là où ce dernier, lorsqu'il est requis[406], devrait être individuel (*cf. supra,* chapitre 2, section 3, B, 3, a).[407] Le consentement collectif constaté dans une convention collective ne peut, selon nous, être assimilé à un consentement individuel.

Il convient de rappeler que la Commission de la protection de la vie privée estime que l'accord des syndicats, bien qu'il signifie dans ce cas un pas en avant, peut difficilement passer pour un consentement des personnes concernées[408].

---

403 F. HENDRICKX, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 65.

404 Les dispositions contraires aux textes impératifs seront déclarées nulles en vertu de l'article 9 de la loi.

405 F. HENDRICKX, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 68.

406 Rappelons que l'employeur est en principe apte à édicter des règles d'utilisation des outils informatiques et au contrôle de ceux-ci. Le consentement du travailleur sera néanmoins parfois nécessaire dans certains cas, comme celui de la prise de connaissance de communications électroniques.

407 Voy. Les développements très complets de F. HENDRICKX, *Privacy en arbeidsrecht*, pp. 63-68, concernant la convention collective et pp. 68 à 70, concernant le règlement de travail.

408 Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be.

225. Ceci dit, le Groupe de l'Article 29 rappelle que la légitimité de ces opérations de traitement ne doit pas reposer exclusivement sur le consentement du travailleur, qui doit être une « manifestation de volonté libre » aux termes de la directive 95/46/CE. Ainsi, le Groupe de l'Article 29 estime-t-il que la question du consentement doit être envisagée dans une perspective plus large : l'implication de toutes les parties prenantes par le biais de conventions collectives pourrait ainsi constituer une façon adéquate de considérer les finalités de traitement comme légitimes[409].

En outre, de telles conventions collectives peuvent, selon la Commission de la protection de la vie privée, être considérées comme des compléments à l'obligation d'information reprise à l'article 9 de la loi du 8 décembre 1992[410].

d. Directives, notes internes et pratiques

226. Les directives et notes internes données au travailleur n'impliquent certes pas que le travailleur y a consenti.

Certaines pratiques et techniques mises en place parallèlement à la règlementation permettent toutefois au travailleur de marquer son consentement sur certaines politiques de contrôle ou sur l'utilisation de certaines technologies. Ainsi, on a déjà évoqué la possibilité qui serait offerte au travailleur de refuser sa géolocalisation en bloquant cette fonctionnalité sur son terminal, ou encore d'indiquer qu'il accepte que ses e-mails entrants soient lus par un autre membre du personnel.

Mentionnons également qu'il a déjà été jugé en jurisprudence qu'un consentement pouvait être implicite et ressortir des pratiques de l'entreprise, ou de l'attitude du travailleur. Nous nous référons à cet égard à l'arrêt déjà évoqué de la Cour du travail d'Anvers qui considère qu'il y a consentement suite à l'autorisation « implicite » faite par une employée à un de ses collègues de consulter sa messagerie pendant son absence. Il déboute cette dernière de son action suite à son licenciement pour motif grave après avoir admis que l'employeur accède aux e-mails de son employée pendant son absence afin d'assurer la continuité de l'entreprise, en considérant que le fait que la travailleuse ait communiqué le mot de passe de sa boîte e-mail impliquait l'acceptation d'un tel accès[411].

---

409 Groupe de l'Article 29, Avis 5/2005 sur l'utilisation de données de localisation aux fins de fourniture de services à valeur ajoutée, 25 novembre 2005, 2130/05/FR, WP115, www.europa.eu/comm/privacy.

410 Commission de la protection de la vie privée, Avis 12/2005 relatif à une proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, 7 septembre 2005, www.privacycommission.be.

411 C. trav. Anvers, 8 janvier 2003, A.R., nº 2020255, www.cass.be ; *contra :* Trib. trav. Verviers, 20 mars 2002, *J.T.T.,* 2002, p. 183 qui considère que l'accès à l'ordinateur d'un travailleur en son absence ne relève pas

La difficulté que pose cet arrêt consiste, selon nous, dans la validité du consentement du travailleur, lorsque celui-ci est requis, face aux critères que ce consentement est sensé respecter (libre, spécifique, informé, individuel et préalable).

G. Déclaration du traitement

227. Le traitement entrepris par l'employeur devra faire l'objet d'une déclaration auprès de la Commission de la protection de la vie privée, en vertu de l'article 17 de la loi du 8 décembre 1992. En effet, les articles 51 à 62 l'arrêté royal du 13 février 2001[412], prévoyant une exemption de déclaration pour certaines catégories de traitements, ne nous semble pas s'appliquer pour les traitements de données n'ayant pas pour seule finalité la gestion du personnel, entendue au sens strict.

Dès lors, tout traitement de données susceptible de permettre le contrôle des travailleurs devra faire l'objet d'une déclaration auprès de la Commission de la protection de la vie privée.

Conclusion

228. En conclusion, nous ne pouvons que constater que la matière se révèle d'une grande complexité, et ceci pour plusieurs raisons.

En premier lieu, la multitude de textes éparses entraîne que l'ensemble des dispositions appelées à régir le contrôle des travailleurs sont parfois contradictoires ou à tout le moins difficilement conciliables. En effet, comment composer avec une convention collective qui déroge à une interdiction posée par la loi ? Comment concilier le principe d'autorité de l'employeur et une impossibilité légale de contrôler le travailleur dans certains cas ?

Ensuite, l'absence de législation spécifique en la matière oblige à aller puiser dans de multiples dispositions des principes qui ne sont pas toujours adaptés à la réalité des relations de travail. On a ainsi pu observer que l'accès aux e-mails d'un employé ayant quitté l'entreprise pouvait se révéler hasar-

---

de l'exercice « normal » de l'autorité d'un employeur. Il nous semble dans tous les cas plus prudent de constater une pratique par écrit dans un document pour éviter les discussions portant sur le caractère « normal » d'une immixtion patronale dans la vie privée d'un travailleur. Constater cette immixtion ne rendra pas pour autant cette immixtion légale ou licite, notamment si le consentement du travailleur était requis.

412 A.R. portant exécution 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, *M.B.*, 13 février 2001.

deuse dès lors que la prise de connaissance de ces e-mails nécessite en principe l'accord de tous les participants à la communication électronique.

Enfin, l'évolution technologique peut parfois rendre certaines dispositions obsolètes ou même inapplicables. Ainsi, la C.C.T. nº 81 se voulait technologiquement neutre, et tentait de régir le contrôle des communications électroniques au sein de l'entreprise. Toutefois, on a vu que le texte de la convention collective n'était pas du tout adapté à la prise de connaissance de communications électroniques ayant généré des données de localisation ou à l'enregistrement de conversations téléphoniques, pourtant considérées comme des communications électroniques au sens de la loi du 13 juin 2005.

229. À l'heure où nous écrivons ces lignes, la Commission de la protection de la vie privée a annoncé qu'elle préparait une recommandation ayant pour objectif de clarifier le cadre existant et de lui donner une interprétation alternative, permettant plus de souplesse et de flexibilité dans les contrôles opérés par les employeurs[413].

Devant ces incertitudes juridiques, il nous semble qu'un texte législatif spécifique serait préférable et permettrait d'y voir plus clair et de régler certaines problématiques non encore résolues. Si des tentatives législatives ont déjà eu lieu[414], il est plus qu'urgent de clarifier le cadre légal régissant le contrôle de l'utilisation des technologies de la communication et de l'information par les travailleurs[415].

Le mot d'ordre concernant la surveillance des travailleurs au moyen des technologies mises à leur disposition est la prévisibilité. On ne peut que regretter que l'arsenal législatif en vigueur ne fasse pas preuve de cette qualité.

---

413 Colloque « Vie privée au travail » organisé à Louvain-la-Neuve le 18 novembre 2010 par l'U.C.L. À l'heure où les auteurs terminent le présent texte, ce texte n'est pas encore rendu public.

414 Voy. Proposition de loi visant à encadrer la surveillance des travailleurs par l'utilisation du système de monitoring associé au système de navigation GPS sur les véhicules de service, dans le respect de la loi du 8 décembre 1992 relative à la protection de la vie privée, ayant fait l'objet d'un avis de la Commission de la protection de la vie privée nº 12/2005 ; voy. également la proposition de loi visant à réglementer l'utilisation des moyens de télécommunication sur le lieu de travail, *Doc. Parl.*, Sénat, session 1999-2003, nos 2-891/1, 29 août 2001 et l'avis nº 39/2001 de la Commission de la protection de la vie privée sur cette proposition du 8 octobre 2001, www.privacycommission.be.

415 Au moment d'achever la rédaction de cette contribution, les auteurs notent une proposition de loi visant à modifier la loi du 13 juin 2005 en vue d'assurer une meilleure protection de la vie privée pour les « services à données de localisation » ou services de « géolocalisation » par téléphone portable a été déposée le 18 novembre 2010 (DOC 53 0615/001).