Le cybercontrôle des travailleurs contrôlé par le Juge

Rosier, Karen

Published in:
Orientations

Publication date:
2009

Document Version
le PDF de l'éditeur

Le cybercontrôle des travailleurs contrôlé par le Juge

Karen ROSIER
Avocate
Chercheuse Senior au Centre de Recherches Informatique et Droit (Crid)
Assistante à la faculté de droit des Facultés Universitaires Notre Dame de la Paix de Namur

Ces dernières années ont vu se multiplier les litiges opposant travailleurs et employeurs à propos la production en justice d'informations recueillies sur l'utilisation de l'e-mail ou de l'internet par le travailleur. L'enjeu n'est pas anodin puisqu'il s'agit généralement pour l'employeur d'établir l'existence de faits justifiant un licenciement pour motif grave, que ces faits résident dans l'usage excessif de ces outils de communication ou de fautes accomplies par le biais de ceux-ci. Nous analyserons dans cet article l'arrêt rendu en la matière par la Cour du travail d'Anvers, le 2 septembre 2008.

1. Tel est pris qui croyait prendre

Le cas tranché par la Cour du travail d'Anvers mêle les deux types de reproches. Un contrôle opéré par le responsable du département I.C.T. de l'entreprise avait révélé qu'un employé avait utilisé une connexion réservée au serveur *mail* de l'entreprise pour ses communications, et ce vraisemblablement dans le but de se soustraire au système de contrôle de l'usage de l'internet et de l'e-*mail* mis en place par l'employeur. Les données récoltées à cette occasion mettent en évidence une utilisation intensive de l'internet et de l'e-*mail* à des fins privées par un employé qui se révéla être, après individualisation des données, un autre membre du département I.C.T. Le contrôle opéré pendant plusieurs jours révèle que ce comportement est systématique, l'analyse des heures de réception et d'envois d'e-*mail*s permettant de surcroît de supposer que la boîte e-*mail* privée du travailleur est constamment ouverte.

L'employeur fait essentiellement état des connexions à des sites internet, des envois d'e-*mails* et du *chat* sur internet à des fins privées pendant les heures de travail mais également du contenu de certaines communications. Il ne se limite donc pas aux données de communications[1]; il a manifestement pris connaissance du contenu de celles-ci. En témoigne le fait qu'il indique dans la lettre de licenciement qu'il a constaté que le travailleur avait expliqué par e-*mail* à une personne tierce à l'entreprise comment installer un programme avec une licence illégale. D'autres éléments relatifs au contenu des communications sont également portés à la connaissance de la Cour.

Le travailleur fait valoir que ce contrôle intervenu fort opportunément quelques jours après qu'il eut demandé et obtenu un congé de paternité, avait été mené de façon illicite.

La cour vérifie, de la mise en place du système contrôle jusqu'à sa mise en œuvre dans le cas d'espèce, si les conditions définies pour la prise de connaissance de la C.C.T. n°81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau[2] ont été respectées.

2. Un cadre légal (trop?) complexe

On gardera toutefois à l'esprit que la C.C.T. n°81 s'inscrit dans un cadre réglementaire pour le moins restrictif en ce qui concerne la possible prise de connaissance des communications électroniques qui incluent tant l'e-*mail*, que les connexions à l'internet et les S.M.S. En effet, contrairement au courrier papier protégé par le secret des lettres, le courrier électronique relève du secret des communications électroniques.
Outre l'application des articles 8 de la C.E.D.H. et de l'article 22 de la Constitution, il y a lieu de tenir compte en cette matière 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). La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel s'applique également 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 relatives à une personne physique. Les principes de cette loi ont d'ailleurs largement inspiré les auteurs de la C.C.T. n°81, comme il est précisé dans le préambule de celle-ci.

L'article 124 de la loi du 13 juin 2005 relatives aux communications électroniques précise 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 quel-

[1] 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, etc.

[2] La C.C.T. n° 81 a été adoptée le 26 avril 2002 et a été rendue obligatoire par arrêté royal du 12 juin 2002.

conque de l'information, de l'identification ou des données obtenues intentionnellement ou non ».

La protection concerne les communications privées, c'est-à-dire les communications qui ne sont pas destinées à être « entendues » –ou plutôt dans le contexte des communications électroniques « lues »– par tout un chacun[3]. 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 »[4].

Aux termes de l'article 124 précité, il est donc interdit notamment 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 autres personnes directement ou indirectement concernées par l'information[5].

Bien que le libellé de l'article 124 de la loi du 13 juin 2005 ne diffère que légèrement de celui de l'article 109*ter*D, et qu'il ne semble pas qu'il ait été dans l'intention du législateur de réformer la portée de la disposition pour étendre la protection au contenu des courriers électroniques (l'article 124, 1° se réfère toujours à l'existence d'une information et non à l'information elle-même), il est permis de penser que cette disposition concerne également le contenu des communications. Le quatrième alinéa de l'article 124 utilise le terme « *information* », suggérant ainsi que l'information elle-même contenue dans le courrier électronique est protégée[6]. Ceci étant, le contenu du courrier électronique est, en toute hypothèse, toujours protégé par les articles 314*bis* et 259*bis* du Code pénal qui n'ont pas été abrogés lors de l'adoption de la loi du 13 juin 2005.

Ces dispositions font donc obstacle, sinon à la prise de connaissance du contenu des communications électroniques, à tout le moins à la prise de connaissance des données de communication. Pour répondre au besoin de contrôle des employeurs, les partenaires sociaux ont négocié la C.C.T. n°81. Le principe qui y est posé est que l'employeur peut déterminer les conditions d'utilisation des outils qu'il met à la disposition de ses travailleurs et donc, le cas échéant en interdire tout usage à des fins privées. Néanmoins, l'employeur ne pourra, même dans ce cas, effectuer un contrôle de cette utilisation des outils sans respecter certaines conditions définies dans la C.C.T. et qui assurent le respect des principes de finalité, de proportionnalité et de transparence dans la mise en œuvre du contrôle.

La C.C.T. offre un cadre très utile pour permettre un certain contrôle de l'employeur de l'utilisation par les employés des moyens de communications électroniques. On peut toutefois s'interroger sur la validité des dérogations aux dispositions légales précitées que la C.C.T. contient. Il nous apparaît 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[7]. En particulier, il nous semble illégal de s'affranchir 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. Ainsi, l'affirmation contenue dans le préambule de la C.C.T. n°81 et aux termes de laquelle « *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* » et l'article 11, al. 3 de la C.C.T. qui en traduit l'application au sein de la C.C.T. sont contraires à l'article 124 de la loi du 13 juin 2005[8].

L'arrêt de la Cour du travail d'Anvers du 2 septembre 2008 concentre son analyse sur le respect de la C.C.T. et n'examine pas le contrôle opéré sous l'angle de l'article 124 de la loi du 13 juin 2005. Pour répondre à l'argumentation du travailleur, elle se prononcera toutefois sur une éventuelle violation de l'article 314*bis* du Code pénal.

3. La régularité du contrôle de l'employeur au regard des dispositions de la C.C.T. n°81

a) Le champ d'application de la C.C.T.

La Cour du travail d'Anvers se prononce, tout d'abord, sur le champ d'application de la C.C.T. En effet, les connexions internet mises en cause avaient été réalisées via une connexion réservée au serveur mail et non au moyen de la connexion internet à la disposition du travailleur pour l'exécution de ses prestations de sorte que le travailleur soutenait que la C.C.T. ne s'appliquait pas. La cour trouve appui sur l'article 2 de la C.C.T. pour considérer 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. En effet, elle relève que l'article 2 de cette convention, relatif au champ d'application de la convention, vise les « *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* ». Elle en conclut que l'interprétation restrictive de l'employé est incompatible avec les termes de la disposition et avec la volonté des auteurs qui en résulte.

Nous en retiendrons donc qu'à partir du moment où le travailleur utilise le matériel de l'entreprise pour faire transiter

---

3 O. RIJCKAERT, « Surveillance des travailleurs: nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 44; Th. VERBIEST et E. WERY, *Le droit de la société de l'information. Droits européen, belge et français*, Bruxelles, Larcier, 2001, p. 188.

4 F. HENDRICKX, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 190; C. trav. Anvers (sect. Anvers), 15 déc. 2004, *Chron. D.S.*, 2006, p. 146.

5 O. RIJCKAERT, « Le contrat de travail face aux nouvelles technologies », *Orientations*, 2000, p. 210. Pour un cas d'application, voy.: C. trav. Bruxelles (3ème ch.), 10 févr. 2004, *Oriëntatie*, 2004, p.3, note A VANOPPEN; *Orientations*, 2006, p. 141.

6 Voy. à ce propos: 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.

7 Voy. en ce sens: O. RIJCKAERT, « Surveillance des travailleurs : nouveaux procédés, multiples contraintes », *Orientations*, n° spécial 35 ans, mars 2005, p. 43; J.F. NEVEN, « Les principes généraux: les dispositions internationales et constitutionnelles », *in Vie privée du travailleur et prérogatives patronales*, Bruxelles, E.J.B.B., 2005, p. 44.

8 Voy. en ce sens: C. trav. Anvers (sect. Anvers), 15 déc. 2004, *Chron. D.S.*, 2006, p. 146.

une communication électronique, la convention s'applique. C'est d'ailleurs en ce sens que le Tribunal du travail de Liège avait considéré 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[9].

b) Transparence, finalité et proportionnalité: les principes clés de la C.C.T.

La cour s'en tient aux principes posés par la C.C.T., à savoir les principes de finalité, de proportionnalité et de transparence. Ces trois principes concrétisés par différentes dispositions de la C.C.T. sont interdépendants. Ainsi, la prise de connaissance des données de communications des travailleurs ne peut-elle intervenir que pour certaines finalités limitativement énumérées par l'article 5 de la C.C.T. Tant le principe que les modalités et finalités des contrôles doivent préalablement être communiqués aux travailleurs par le biais d'une information collective et d'une information individuelle conformément aux articles 7 à 9 de la C.C.T., ce qui assure la transparence du contrôle.

Par ailleurs, les modalités définies pour la mise en œuvre du contrôle sont, pour traduire l'exigence de proportionnalité dans le contrôle, fonction de la finalité poursuivie comme précisé aux articles 11 à 17 de la C.C.T. Ainsi, si la C.C.T. permet une individualisation immédiate des données pour identifier l'auteur du comportement problématique, elle exclut toutefois cette possibilité lorsque le contrôle vise à vérifier que les travailleurs respectent les consignes de l'employeur relatives à l'utilisation des outils de communication. Dans ce cas, l'employeur doit informer les travailleurs de l'existence de l'anomalie et les avertir qu'une individualisation des données de communication électroniques aura lieu si l'anomalie se répète[10].

c) Les exigences relatives à l'information

La cour évoque qu'à plusieurs reprises le travailleur licencié avait été informé des règles applicables, et ce tant en ce qui concerne les modalités de contrôles que les règles définies par l'employeur pour l'utilisation de l'*e-mail*. En effet, le règlement I.T. de l'entreprise précisait que l'utilisation de l'internet et de l'*e-mail* à des fins privées sans l'autorisation expresse de l'employeur n'était tolérée que pendant les périodes de pause ou pour des raisons familiales impérieuses. La cour relève que le règlement I.T. avait été communiqué aux travailleurs au moment de son adoption en février 2005 et avait fait l'objet de séances d'information spécifiques. Elle relève que le 1er mars 2005, le personnel de surveillance avait envoyé un *e-mail* collectif attirant l'attention des travailleurs sur le fait que ce règlement devait être respecté. Le travailleur licencié ne pouvait donc ignorer le règlement et son application effective lors du contrôle opéré en septembre 2005.
Le travailleur avait toutefois fait valoir que, sans en avoir averti son personnel, l'entreprise utilisait un système dont une fonctionnalité permettait à tout moment une individualisation du contrôle de sorte qu'il était illusoire de penser que l'entreprise s'en prive, quelle que soit par ailleurs la finalité du contrôle. La Cour considère que l'employeur n'a pas à informer les travailleurs de tous les détails techniques relatifs aux modalités de contrôle. Le texte de la C.C.T. autorise cette interprétation dans la mesure où si, tant à l'article 7 qu'à l'article 8, la C.C.T. indique expressément que l'information doit porter sur tous les aspects du contrôle, ceux-ci, spécifiquement énumérés à l'article 9, ne portent que sur 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, le lieu et la durée de conservation ainsi que sur le caractère permanent ou non du contrôle.

En revanche, on constatera que la cour ne se prononce pas sur la question du respect de l'information collective des travailleurs. D'autres juridictions avaient considéré l'absence de preuve de cette information préalable dans le cadre de l'application de la C.C.T. n°68[11] –qui comporte une obligation similaire– comme entachant d'irrégularité tout contrôle[12].

d) Les finalités du contrôle et les modalités de celui-ci

La cour retient qu'en l'espèce, le responsable I.C.T. qui avait opéré le contrôle avait commencé par repérer une utilisation suspecte, dans le chef de plusieurs travailleurs, des ressources informatiques de l'entreprise de par l'utilisation d'une connexion et un *firewall* nouvellement installé. Il s'agissait donc de vérifier le bon fonctionnement du réseau, ce qui correspond à une finalité de contrôle expressément autorisée par l'article 5, § 1er, 3° de la C.C.T. Il est apparu au responsable I.C.T., dans un second temps, que le trafic internet était particulièrement élevé pour un seul de ces travailleurs, en l'occurrence l'employé licencié par la suite. La cour relève à cet égard qu'un contrôle visant à vérifier le respect du règlement I.T. de l'entreprise –qui ne permettait qu'un usage exceptionnel de l'internet à des fins privées en dehors des périodes de pause– était également possible au regard de l'article 5, § 1er, 4° de la C.C.T. La cour constate explicitement que le règlement I.T. prévoyait un possible contrôle des communications des travailleurs dans le but de vérifier le respect de ses dispositions par ceux-ci.

L'un des motifs du licenciement résidait dans le fait que le travailleur n'avait pas respecté les modalités d'utilisation de l'*e-mail* et de l'internet prescrites par le règlement I.T. en vigueur dans l'entreprise. L'employeur invoquait à l'appui de ce grief les données récoltées lors du contrôle mettant en évidence ce non-respect. Le travailleur faisait toutefois grief d'avoir procédé, lors du contrôle, à une individualisation des données sans phase d'information préalable, ce qui n'était pas contesté. La description du déroulement du contrôle

---

9 Trib. trav. Liège (3e ch.), 19 mars 2008, RG 360.454, www.cass.be.

10 C.C.T. n°81, art. 16.

11 C.C.T. n°68 du 16 juin 1998 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, rendue obligatoire par AR. du 20 septembre 1998.

12 Voy. à cet égard l'arrêt de la Cour du travail de Bruxelles du 15 juin 2006 qui relève que, pour respecter les obligations d'information prescrites à l'article 9, §§ 1er et 4 de la C.C.T. n°68, il ne suffit pas d'informer le conseil d'entreprise quant à la finalité des caméras utilisées par l'employeur ; encore faut-il que l'employeur puisse démontrer qu'il avait informé le conseil d'entreprise du principe du placement des caméras dès avant leur installation (C. trav. Bruxelles (2e ch.), 15 juin 2006, *J.T.T.*, 2006, p. 392, note).

met de fait en évidence que le responsable I.C.T. a, parmi les travailleurs qui utilisaient la connexion suspecte, choisi de poursuivre ses investigations à l'égard de l'un d'entre eux en raison de la quantité de trafic révélant une violation du règlement I.T.

La cour estime, d'une part, qu'il n'était pas « déraisonnable » qu'après avoir identifié un groupe de travailleurs utilisant une connexion suspecte, le responsable I.C.T. étudie de plus près les connexions réalisées par le travailleur qui en faisait un usage intensif. La cour indique, d'autre part, 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.

A suivre la cour, le simple fait que le contrôle vise au moins une finalité pour laquelle aucune phase d'alerte préalable n'est exigée autoriserait une identification immédiate du contrevenant, et ce nonobstant les conséquences que l'on pourrait tirer par la suite du constat d'une éventuelle violation des règles d'utilisation internes à l'entreprise dans le chef de la personne identifiée.

Cette conclusion est critiquable tant il serait aisé de contourner l'exigence d'une mise en garde préalable en justifiant que le contrôle n'est pas seulement destiné à contrôler le respect des directives d'utilisation des outils de communication mais également mené pour repérer un dysfonctionnement du réseau.
La C.C.T. nous semble d'ailleurs reposer sur des principes incompatibles avec cette interprétation. L'article 14 de la C.C.T. prévoit expressément que « *L'employeur ne peut individualiser les données de communication électroniques en réseau collectées lors d'un contrôle, d'une manière incompatible avec le ou les finalités poursuivies et visées à l'article 5, § 1er* » et que « *Sont individualisées les données de communication électroniques en réseau nécessaires à la ou les finalités poursuivies pour le contrôle. Elles doivent être adéquates, pertinentes et non excessives au regard de cette ou ces finalités* ». Il en résulte que la possibilité d'individualiser des données est indissociable de la finalité du contrôle dans laquelle elle s'inscrit. Aussi, si en vue d'assurer le bon fonctionnement du réseau, le personnel de surveillance peut individualiser les données pour mettre fin à un comportement nuisant à ce bon fonctionnement, les données individualisées ne peuvent être utilisées que dans cet objectif. L'individualisation qui s'inscrit dans un objectif de contrôle du respect des modalités d'utilisation définies par l'employeur nous apparaît requérir une mise en garde préalable des travailleurs.

Notons encore que, toujours concernant les modalités de contrôle, le travailleur invoquait que le système de contrôle mis en place ne permettait pas techniquement à la personne qui exerçait la surveillance de n'avoir accès qu'aux données de connexion sans le contenu des communication. On peut effectivement comprendre la pertinence de l'argument puisque la C.C.T. ne permet en toute hypothèse que la prise de connaissance des données de communications à l'exclusion du contenu[13]. La cour estime toutefois qu'il ne s'agit là que d'une conséquence technique secondaire du système utilisé qui n'est pas disproportionnée au regard de la finalité poursuivie, à savoir la vérification du fait que les travailleurs respectent les modalités d'utilisation définies dans le règlement I.T. de l'entreprise.

Elle estime expressément, par ailleurs, que c'est à bon droit que l'employeur a valablement pris connaissance lors du contrôle du contenu des *e-mails* de l'employé en se conformant uniquement à la C.C.T. et aux dispositions du règlement I.T. de l'entreprise. Ceci repose la question de la légalité des contrôles au regard du cadre législatif applicable et rappelé ci-avant. La cour n'envisage toutefois que partiellement cette question, pour répondre à un argument soulevé par le travailleur concernant le non-respect de l'article 314*bis* du Code pénal.

4. La régularité du contrôle au regard de l'article 314*bis* C.P. et 124 de loi du 13 juin 2005

L'article 314*bis* du Code pénal prescrit une interdiction, sauf consentement de toutes les parties à la communication, de prendre intentionnellement connaissance du contenu des communications pendant leur transmission et de détenir, révéler ou divulguer à une autre personne le contenu de communications ou de télécommunications privées, illégalement « écoutées » ou enregistrées, ou dont il a pris connaissance illégalement, ou d'utiliser sciemment d'une manière quelconque une information obtenue de cette façon.

Le travailleur invoquait qu'il y avait eu violation de l'article 314*bis* du Code pénal.

La protection relative au contenu des communications électroniques n'intervient que pendant la transmission. Dès lors que la transmission du courrier électronique est achevée, la protection du contenu n'existe plus[14]. C'est précisément l'un des arguments retenus par la Cour du travail d'Anvers pour conclure à l'absence d'infraction dans l'affaire tranchée.
La cour estime, de surcroît, qu'en l'espèce, le travailleur ayant accepté l'éventualité d'un contrôle des communications transitant sur le réseau et via l'équipement de l'entreprise, l'élément moral de l'infraction ferait défaut. Le travailleur avait dû signer un document par lequel il marquait son accord avec les dispositions du règlement I.T. de l'entreprise. La cour estime que, dans ces conditions, on ne peut soutenir que l'élément moral de l'infraction est présent en l'espèce.

Ce raisonnement nous laisse perplexe dès lors que tant l'article 314*bis* du Code pénal que la notion de dol général[15] requièrent l'intention de poser l'acte, le rôle du consentement de la personne concernée étant clairement envisagé par ailleurs dans la définition de l'infraction. En effet, l'infraction n'existe que lorsque la prise de connaissance intervient sans le consentement de toutes les parties à la communication. Autrement dit, s'il est établi que le travailleur

[13] La C.C.T. précise ne pas porter sur la prise de connaissance du contenu des communications qui reste donc principalement régie par les articles 124 de la loi 13 juin 2005 et par l'article 314*bis* du Code pénal.

[14] Pour des applications de ce principe, voy.: C. trav. Anvers (sect. Anvers), 8 janv. 2003, *Chron. D.S.*, 2003, p. 193; *R.W.*, 2005-2006, p. 391; Trib. trav. Bruxelles (3e ch.), 16 sept. 2004, *J.T.T.*, 2005, p. 61.

[15] F. Tulkens et M. van de Kerkhove relèvent que le dol général est la volonté de commettre l'acte interdit ou d'omettre l'acte prescrit par la loi (F. TULKENS et M. VAN DE KERKHOVE, *Introduction au droit pénal*, Bruxelles, Kluwer, 2005, p. 384).

a valablement consenti à la prise de connaissance de ses informations, ceci ne permettrait de conclure à l'absence d'infraction que pour les communications pour lesquelles il n'y a pas d'autres parties à la communication.

En ce qui concerne le caractère **intentionnel** de la prise de connaissance des informations protégées, la jurisprudence tend à la distinguer la prise de connaissance **fortuite**. Dans un jugement du 4 décembre 2007, le Tribunal du travail de Bruxelles distingue la découverte fortuite d'un *e-mail* avec la consultation délibérée d'une telle communication[16]. Se fondant sur l'article 124 de la loi du 13 juin 2005 relative aux communications électroniques qui sanctionne la prise de connaissance intentionnelle de l'existence d'une information de toute nature transmise par voie de communication électronique par une autre personne que son destinataire, le tribunal 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. Le tribunal constate 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[17]. Dans un arrêt du 28 novembre 2006, la Cour du travail de Bruxelles estime que la prise de connaissance de données par un informaticien intervenue incidemment lors d'un *back up* de données lorsque ce dernier se rend compte qu'il existe un fichier de taille inappropriée et l'ouvre est une prise de connaissance involontaire[18].

Ceci étant, même le constat de la non-application de l'article 314*bis* du Code pénal ne suffit pas à justifier que l'employeur fasse état du contenu de certaines communications, comme ce fut le cas en l'espèce. Comme rappelé ci-avant, l'article 124 de la loi du 13 juin 2005 prévoit, en l'absence du consentement de toutes les parties à la communication, l'interdiction de stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non en matière de communications électroniques.

5. Conséquences d'une éventuelle irrégularité du contrôle

La Cour du travail d'Anvers indique, par ailleurs que, à supposer même qu'il y ait eu une irrégularité dans la procédure d'information, celle-ci n'entacherait pas la fiabilité de la preuve ni ne priverait le travailleur d'un procès équitable. Elle entend ainsi faire application de la jurisprudence dite « Antigone » de l'arrêt de la Cour de cassation dans un litige social pour prendre en compte une preuve obtenue éventuellement de manière irrégulière. La cour cite en effet un arrêt de la Cour de cassation du 10 mars 2008 qui applique la jurisprudence de non rejet automatique de la preuve obtenue illicitement jusqu'alors réservée à des litiges en matière pénale à un litige social[19].
Si on peut s'interroger sur la portée de cet arrêt du 10 mars 2008 rendu dans un litige de sanction administrative de suspension d'allocations de chômage par l'O.N.Em. sur la jurisprudence de contentieux des relations de travail[20], force est de constater que la Cour du travail d'Anvers n'est pas la seule à l'avoir invoquée dans ce type de contentieux. Le Tribunal du travail de Gand y fait également référence dans une décision relative à la preuve d'un motif de licenciement du 3 septembre 2008[21].
Cette jurisprudence n'implique pas uniquement que le Juge puisse tenir compte de preuve recueillie irrégulièrement au regard des circonstances et critères dégagés par la Cour de cassation mais lui impose d'évaluer la recevabilité de la preuve au regard de ces critères et de justifier, le cas échéant, pour quels motifs il décide d'écarter une preuve.

6. Conclusion

L'arrêt de la Cour du travail d'Anvers est à l'image de l'évolution de la jurisprudence rendue depuis plusieurs années en matière de contrôle des *e-mails* et de l'usage de l'internet par l'employeur. En effet, les premiers arrêts étaient résolument tournés vers une pondération des droits en présence, à savoir droit de l'employeur à exercer sa prérogative de contrôle, du reste indissociable de ses responsabilités en tant qu'employeur, et droit du travailleur à voir sa vie privée respectée sur le lieu du travail. Par la suite, la jurisprudence s'est davantage attachée à évaluer la recevabilité des preuves soumises au regard des dispositions régissant le secret des communications électroniques.

L'entrée en vigueur de la C.C.T. n°81 a fourni un nouveau cadre de référence, non seulement aux protagonistes que sont les employeurs et les travailleurs, mais également à la jurisprudence. Les décisions les plus récentes se limitent dès lors à un contrôle de la légalité de la collecte de la preuve au regard de la C.C.T. qui permet une approche plus pragmatique de la problématique. Celle-ci transparaît, à notre estime, dans l'arrêt commenté, et ce parfois au détriment de la rigueur des principes.

La solution dégagée prête, en effet, le flanc à la critique en raison de la subsistance d'un cadre légal très strict auquel la C.C.T. n°81 n'offre pas d'alternative adéquate d'un point de vue légal. On ne peut que déplorer cette situation de flou juridique inconfortable tant pour les travailleurs que pour les employeurs. L'éventuelle application de la jurisprudence de la Cour de cassation relative au non rejet automatique de la preuve recueillie de manière irrégulière dans les litiges sociaux n'est pas non plus de bon augure puisqu'elle offre nouveau un terrain de discussion, cette fois sur le sort à réserver aux preuves dont il serait établi qu'elles ont été recueillies irrégulièrement.

---

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

17 Voy. également la décision du Tribunal du travail de Liège du 19 mars 2008 qui considère que le fait de consulter plusieurs *e-mails* et de les imprimer est le fruit d'une démarche active révélatrice d'une intention dans le chef de son auteur (Trib. trav. Liège (3e ch.), 19 mars 2008, RG 360.454, www.cass.be).

18 C. trav. Bruxelles (4e ch.), 28 nov. 2006, *Chron. D.S.*., 2009, p. 32.

19 Cass., 10 mars 2008, *J.L.M.B.*., 2009, p.580, note R. DEBAERDEMAEKER.

20 R. Debaerdemaeker relève que, devant les juridictions de fond, il avait été plaidé par l'O.N.Em. que la sanction participait de sa mission de faire respecter la législation en matière sociale tendant à assimiler les violations à cette réglementation à des infractions pénales (R. DEBAERDEMAEKER, « Admissibilité de la preuve illicitement recueillie: quand la fin justifie les moyens… », note sous Cass., 10 mars 2008, *J.L.M.B.*., 2009, p. 585).

21 Trib. trav. Gand, 1er sept. 2008, R.G 175054/06, www.cass.be.