RAPPORT

établi à l'initiative de la Commission de la protection de la vie privée (ci-après la Commission) ;

présenté et débattu lors de la séance de 6 juillet 2011 de la Commission ;

soumis par la Commission à la consultation publique entre le 15 juillet 2011 et le 30 novembre 2011, afin de permettre aux responsables du traitement et aux personnes concernées de faire valoir leurs observations, remarques ou objections ;

en vue d'adresser aux partenaires sociaux, aux organes de concertation qu'ils constituent et de manière générale à tous les employeurs et travailleurs, des

RECOMMANDATIONS

visant à concilier les prérogatives de l'employeur avec la protection des données à caractère personnel des travailleurs ou de tiers lors de l'utilisation, de la surveillance et du contrôle des outils informatiques de communication électronique dans le cadre de la relation de travail.

I. INTRODUCTION

I.1. CONTEXTE DES RECOMMANDATIONS

1. Le contrôle par les employeurs des outils informatiques utilisés par leurs travailleurs, et surtout des informations qui y transitent ou qui y sont stockées, est un problème complexe et récurrent, qui reste d'actualité.

2. L'attention s'est essentiellement focalisée sur la prise de connaissance de communications électroniques, qu'il s'agisse de la mise en place de procédures ou de procédés visant à exercer une surveillance de ce que se passe sur l'équipement ou le réseau de l'employeur ou de contrôles ponctuels se traduisant par un accès à des informations stockées sur l'équipement. En témoignent les très nombreuses interpellations et demandes d'informations à cet égard adressées à la Commission, tant par les employeurs que par les représentants des travailleurs, ainsi que les plaintes dont elle est régulièrement saisie.

3. On constate que les agissements et comportements personnels des travailleurs (privés ou sans rapport avec le cadre professionnel), de plus en plus souvent liés à l'Internet et à des produits et services virtuels, peuvent se prolonger dans le cadre de leur travail ou via l'utilisation des outils de travail. Cette extension est notamment due à la globalité de l'accès des sites Internet qu'ils visitent. Les travailleurs communiquent, s'informent ou se détendent grâce à l'outil de travail de leur employeur. Elle provient également de la mise à disposition d'outils de travail portables (tels des ordinateurs) que le travailleur utilise en dehors des heures de travail, que cela soit ou non autorisé, voire toléré par l'employeur (de manière comparable à la mise à disposition d'un véhicule de la société).

4. Il convient toutefois de constater d'emblée que l'accès aux courriers électroniques et données de communication Internet ne relève pas uniquement d'une question de surveillance mais également de la gestion des informations et de l'organisation de l'activité de l'employeur : il s'agit notamment de s'assurer de la conservation des correspondances (archivage) mais également de permettre une continuité des activités en cas d'absence, de décès du travailleur ou de départ de celui-ci.

5. Le travailleur, en exécution de son contrat de travail, communique par voie électronique avec des tiers grâce au système informatique géré par son employeur ou à tout le moins, au nom de son employeur.

6. L'employeur a un intérêt légitime à pouvoir accéder à ces informations. Le produit du travail accompli par le travailleur doit en principe être livré à l'employeur selon les règles qu'il fixe. Ce peut être notamment le cas lorsque ces informations forment le contenu de communications (électroniques ou autres) ou renseignent sur des communications (la durée, le destinataire,…) effectuées en exécution du travail convenu et au nom de l'employeur (de manière expresse ou non, dès lors que l'intervention du travailleur est dépourvue d'ambiguïté pour son correspondant et pour lui-même). L'employeur devrait pouvoir recevoir et obtenir ces informations, ou à défaut les rechercher pour en prendre connaissance. Une prise de connaissance de ces informations sans l'intermédiaire du travailleur ne peut toutefois être

considérée comme la manière habituelle de recueillir le produit du travail accompli. En principe, celles-ci sont livrées par le travailleur.

7. Quelle que soit la situation, la question demeure la même : le travailleur peut-il invoquer les dispositions 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* (loi vie privée ou LVP) (et d'autres normes, notamment celles régissant le secret de la correspondance) pour empêcher l'employeur d'accéder à ces informations, par exemple pour contrôler la qualité de son travail et empêcher toute surveillance et tout contrôle des actes qu'il pose via les outils mis à sa disposition ?

8. La réponse à cette question reste controversée, comme en témoignent des divergences de la jurisprudence, les hésitations de professionnels, même spécialisés, et le malaise exprimé par les parties directement concernées.

9. Cette complexité est due aux diverses normes légales qui trouvent à s'appliquer en matière de prise de connaissance des communications électroniques et des données de communication dont l'utilisation par les travailleurs est toutefois de plus en plus répandue.

I.2. CONTENU ET DESTINATAIRES DES RECOMMANDATIONS

10. La Commission souhaite informer les employeurs et les travailleurs, et également les partenaires sociaux et les organes de concertation qu'ils constituent, sur les règles en matière de protection des données à caractère personnel des travailleurs, à l'occasion de la mise en œuvre de traitements qui ont trait à la gestion et au contrôle de l'utilisation de l'outil informatique par les travailleurs. Elle restreindra ses réflexions aux communications électroniques que sont les courriers électroniques et les connexions Internet et n'abordera donc pas la problématique du contrôle des communications téléphoniques, des sms ou encore de la géolocalisation. Il sera fait référence aux communications elles-mêmes (à savoir le contenu d'un e-mail ou d'une page web consultée) et aux données de communications électroniques (adresses des destinataires et expéditeurs, date et heures d'envoi/de réception ou de connexion, adresse des sites Internet consultés).

11. La plupart des données générées par les outils de travail électroniques mis à disposition des travailleurs sont sauvegardées, voire même copiées sur un autre support à des fins de back-up. Il en est ainsi non seulement des documents mais également des données de communications électroniques.

12. La Commission entend se pencher sur les conditions dans lesquelles ces données peuvent être ainsi sauvegardées pour certaines finalités et les conditions dans lesquelles il peut y être accédé, que ce soit dans le cadre d'un contrôle ou d'une surveillance, ou d'une autre finalité. La Commission utilisera dans la suite des présentes recommandations le concept d'accès pour se référer non seulement au fait d'accéder à des données relatives au travailleur mais également aux différentes opérations subséquentes qui s'inscriront dans le cadre du traitement (telle la consultation des données et leur utilisation (impression sur un support papier, transmission à un autre destinataire, etc.)), et ce quelle que soit la finalité poursuivie. Cet accès peut se concevoir tant sur un poste informatique utilisé par un travailleur

que sur d'autres supports sur lesquels les données sont sauvegardées (serveur, supports de sauvegarde, etc.).

13. La Commission rappellera les normes applicables. Elle entend, à l'occasion des présentes recommandations, réexaminer ses positions antérieures en appréciant l'application de toutes ces normes pertinentes à la lumière des dispositions de la LVP[1] (cf. Section II) et évoquera également la question de la régularité de la preuve recueillie au mépris des dispositions applicables (cf. Section III).

14. La Commission formulera, par ailleurs, sous la forme de recommandations, une série de bonnes pratiques, prudentes et diligentes, qui constituent autant d'exemples ou de moyens de tenir compte de la LVP, et qu'elle considère à même de prévenir les conflits entre les intérêts des employeurs et la protection des droits des travailleurs. Celles-ci feront toutefois l'objet d'un document distinct (voir annexes).

15. De manière générale, et sous réserve des conditions de leur mise en œuvre, ces recommandations, dans leur ensemble, doivent permettre de garantir l'adéquate protection des droits et libertés fondamentaux des personnes dont les données à caractère personnel sont traitées lors d'un accès à des communications électroniques.

16. La Commission tient toutefois à préciser que ces recommandations n'ont aucun caractère impératif ou obligatoire. Si leur adoption permet de présumer le respect de la loi, ou à tout le moins la bonne foi du responsable du traitement, leur non-respect ou l'adoption de pratiques différentes ne constituent pas nécessairement une infraction, dès lors qu'il peut être établi que les obligations mises à charge des responsables du traitement ont bien été exécutées par d'autres voies, peut-être plus adaptées à la spécificité de certaines entreprises ou de certaines fonctions.

17. La Commission n'entend pas, à cet égard, se substituer aux employeurs, responsables des traitements de données à caractère personnel effectués par exemple lors du contrôle ou de la surveillance de leurs travailleurs, ni aux partenaires sociaux, qui souhaiteraient négocier et de convenir, dans le respect des lois impératives, des règles organisant l'accès aux communications électroniques.

18. Par ailleurs, ces recommandations sont formulées sans préjudice de l'application d'autres dispositions légales ou réglementaires au respect desquelles sont éventuellement tenus les employeurs,

[1] La Commission s'est prononcée plusieurs fois sur la problématique du contrôle des communications électroniques au travail, en d'autres termes, du contrôle que l'employeur exerce sur l'utilisation du mail et d'Internet par son personnel, notamment par exemple dans l'avis d'initiative n° 10/2000 *relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail*, l'avis d'initiative n° 39/2001 du 8 octobre 2001 *concernant la proposition de loi 2-891/1 du 29 août 2001 visant à réglementer l'utilisation des moyens de télécommunication sur le lieu de travail*, l'avis n° 13/2003 du 27 février 2003 relatif au *contrôle par l'employeur des données de communication de l'un de ses employés*, l'avis n° 47/2003 du 18 décembre 2003 relatif au *code de bonne conduite à l'intention des membres du personnel du Ministère de la Communauté flamande*, l'avis n° 18/2005 du 9 novembre 2005 *relatif à un projet d'arrêté du Gouvernement de la Communauté française relatif au code de bonne conduite des usagers des systèmes informatiques, du courrier électronique et d'Internet au sein des services du Gouvernement de la Communauté française, et des organismes d'intérêt public relevant du comité de secteur XVII* et l'avis n° 21/2006 du 12 juillet 2006 *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*.

telles les dispositions de la CCT n°81 pour ce qui concerne les employeurs non soumis à la loi du 5 décembre 1968 sur les conventions collectives et commissions paritaires.

I.3. PROCÉDURE

19. Le présent document sera soumis par la Commission à une consultation publique du 15 juillet 2011 au 30 novembre 2011 afin de permettre aux responsables du traitement et aux personnes concernées d'exprimer leurs observations, remarques ou critiques, et ce en vue d'adresser aux partenaires sociaux, aux organes de concertation qu'ils ont créés et, de manière générale, à tous les employeurs des recommandations visant à concilier les prérogatives patronales et la protection des données à caractère personnel des travailleurs ou des tiers lors de l'utilisation, de la surveillance et du contrôle des moyens de communications électroniques et informatiques dans le cadre de la relation de travail.

II. CADRE JURIDIQUE

20. La section ci-après reprend un exposé de la législation (au sens large) qui régit le droit de contrôle d'un employeur de l'utilisation des moyens de communication électroniques faite par les travailleurs au travail. Tout d'abord, la discussion portera sur les sources de droit internationales, dont l'article 8 de la CEDH constitue la principale, suivies de la législation belge, avec une analyse des points problématiques du droit de contrôle de l'employeur.

II.1. NORMES INTERNATIONALES

21. Plusieurs dispositions (internationales) régissent le droit au respect de la vie privée d'un travailleur au travail et la protection des télécommunications du travailleur (au travail). Le droit de contrôle de l'employeur y est également lié.

22. La norme internationale la plus importante à ce sujet est reprise à l'article 8 de la CEDH, qui garantit le droit à la protection de la vie privée et familiale, du domicile et de la correspondance, et stipule que :

"1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui."

23. La Cour européenne des Droits de l'Homme a déjà confirmé dans plusieurs arrêts que la protection de la vie privée, telle que définie à l'article 8 de la CEDH, s'applique également au sein d'une

entreprise[2]. L'arrêt *Copland* contre le Royaume-Uni est intéressant[3]. Cet arrêt traite de la plainte d'une enseignante dont le téléphone avait été mis sur écoute et l'utilisation de la messagerie électronique et d'Internet contrôlée par son employeur, sans aucun consentement préalable de la part de l'intéressée. La Cour a jugé que les appels téléphoniques passés depuis les locaux professionnels étaient à première vue couverts par les notions de "vie privée" et de "correspondance" au sens de l'article 8 de la CEDH. Il en va de même pour les courriers électroniques ou les informations relatives aux sites Internet consultés par un travailleur. Il en résulte qu'à défaut d'un avertissement relatif au contrôle dont il peut faire l'objet, le travailleur peut avoir une confiance légitime quant au caractère privé de ces données, de sorte que la collecte et le traitement des données citées constitue une ingérence dans les droits garantis par l'article 8 de la CEDH. Toujours selon la Cour, le fait que ce contrôle serait limité à un relevé des dates et heures des appels effectués, ainsi qu'à l'identification des numéros composés importe peu. La Cour juge ici que cela est contraire à la CEDH, notamment vu l'absence de toute législation régulant de telles pratiques, mais elle ajoute que si une telle législation avait existé, un contrôle aurait été permis s'il avait été nécessaire dans une société démocratique, et ce "dans certaines situations". En tout cas, au regard de l'arrêt *Copland*, il est clair que l'affirmation selon laquelle il n'est plus question de protection de la vie privée dès que l'on se trouve sur le lieu de travail et que l'on utilise les équipements de l'employeur n'est pas défendable.

24. La Cour européenne a déjà précisé dans l'arrêt *Copland* qu'une restriction était en effet possible sous certaines conditions. On peut notamment déduire du texte de l'article 8 de la CEDH qu'une violation du droit au respect de la vie privée est permise lorsque les conditions suivantes sont remplies :

- la violation (est conforme à une norme existante, claire et accessible (*principe de légalité*) ;
- l'employeur doit avoir une finalité légitime, à savoir la nécessité de protéger un droit fondamental (*principe de finalité*);
- la violation doit être proportionnelle (*principe de proportionnalité*) : une violation du droit au respect de la vie privée n'est permise que si celle-ci est liée aux finalités pour lesquelles elle a été commise. Dans le cadre de ce contrôle de proportionnalité, le droit au respect de la vie privée peut être mis en balance non seulement avec d'autres droits fondamentaux, mais également, selon HENDRICKX et J.-F. NEVEN, avec les intérêts économiques de l'employeur[4].

25. La Directive européenne n° 95/46 du Parlement européen et du Conseil du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[5] doit également être mentionnée. Cette directive a été transposée en Belgique par une adaptation de la Loi Vie Privée belge, de sorte qu'en tant que telle, cette directive ne fera l'objet d'aucun examen approfondi ci-après.

---

[2] Voir Niemitz c. Allemagne, 23 novembre 1992, *Série A*, vol. 251/B, § 30 et Halford c. Royaume-Uni, 27 mai 1997, *Recueil* 1997-III, § 44.
[3] Copland c. Royaume-Uni, 3 avril 2007, à consulter sur http://www.echr.coe.int.
[4] F. HENDRICKX, *Privacy en arbeidsrecht*, Bruges, Die Keure, 1999, p. 45 ; J.-F. NEVEN, "Les principes généraux : les dispositions internationales et constitutionnelles", in ss. dir. J.-F. LECLERCQ, Vie privée du travailleur et prérogatives patronales, Bruxelles, EJBB, pp. 30-32.
[5] *JO. L*281 du 23 novembre 1995, 31.

26. On peut également faire référence à un recueil de directives pratiques de l'OIT relatives à la protection des données à caractère personnel, adopté lors de la 267ème séance en novembre 1996[6].

27. Enfin, on peut encore se référer aux normes internationales suivantes qui contiennent des dispositions protégeant le droit au respect de la vie privée (mais auxquelles la doctrine et la jurisprudence belges ne font quasiment pas référence) :

- article 17 du Pacte international relatif aux droits civils et politiques (PIDCP) ;
- article 12 de la Déclaration universelle des droits de l'homme ;
- articles 7 et 8 de la Charte européenne des droits fondamentaux ;
- la Directive européenne n° 2002/58 en matière de communications électroniques (cette directive a été transposée en Belgique par la loi du 13 juin 2005 *relative aux communications électroniques*) et la Directive européenne n° 2009/136 en matière de communications électroniques ;
- la Convention n° 108 et le protocole additionnel n° 181 du Conseil de l'Europe ;
- des directives de l'OCDE ;
- des directives des Nations unies.

II.2 PROTECTION BELGE DE LA VIE PRIVEE

1. Droit fondamental repris à l'article 22 de la Constitution

28. L'article 22 de la Constitution prévoit que :

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

29. L'article 22 doit être interprété à la lumière de l'article 8 de la CEDH. En outre, le droit est complété par des dispositions légales telles qu'exposées ci-après.

2. Le secret des communications électroniques

a. Article 314*bis* du Code pénal

30. L'article 314*bis* du Code pénal rend punissable l'écoute, la prise de connaissance ou l'enregistrement de (télé)communications privées pendant leur transmission :

> *"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, 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*

[6] *Protection of workers' personal data. An ILO code of practice*, Genève, OIT, 1997.

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 euros à vingt mille euros 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. (…)" (soulignement propre)

31. Il s'agit ici clairement du contenu des communications. Les communications professionnelles telles qu'un courrier électronique, qui ne sont pas destinées à être écoutées ou lues par d'autres personnes que les correspondants, sont également protégées par cette disposition. Par conséquent, un employeur qui prend connaissance du contenu de courriers électroniques qui ne lui sont pas destinés ou dont il n'est pas l'expéditeur à l'intercession d'un employé et qui sont envoyés ou reçus par ses travailleurs est passible d'une peine.

32. Toutefois, il faut signaler que l'article 314*bis* du Code pénal n'empêche pas, selon certains auteurs, qu'un employeur contrôle la boîte de réception d'un travailleur, étant donné qu'un tel contrôle n'est pas effectué "pendant la transmission" de la communication[7].

33. Une majorité de la jurisprudence semble également partir du principe d'une interprétation stricte de l'article 314bis du Code pénal de sorte que cette disposition ne puisse pas s'appliquer à la consultation d'un courrier électronique d'un travailleur étant donné que cela ne se produit plus "pendant la transmission" du courrier électronique[8].

34. En outre, on peut argumenter que le contrôle de l'utilisation d'Internet, sous la forme d'un enregistrement des sites Internet (ce qu'on appelle "journaliser"), ne relève pas du champ d'application de cette disposition[9].

[7] Voir notamment F. HENDRICKX, Privacy en arbeidsrecht, Bruges, die Keure, 1999, 188-190 ; P. VAN EECKE et J. DUMORTIER, "Bescherming van privécommunicatie op het internet", in S. PARMENTIER (red.), De rechten van de mens op het internet, Anvers, Maklu, 2000, 85.
[8] Voir notamment C.T. Gand, 12 décembre 2007, non pub. et C.T. Gand, 13 mars 2006, non pub. tels que cités dans P. WATERSCHOOT, "Bespreking van enkele arresten van het Arbeidshof te Gent in verband met het gebruik en misbruik van e-mail en internet op de werkplaats en het controlerecht van de werkgever daarop", R.W. 2008-2009, 730 -744 ; C.T. Gand, 9 mai 2005, Soc.Kron. 2006, n° 3, 158.
[9] Voir C.T. Gand, 4 avril 2001, *J.T.T.* 2002, 49.

35. L'article 314*bis* du Code pénal exige que l'on agisse intentionnellement, c'est-à-dire agir sciemment. Une découverte purement fortuite ne sera donc pas punissable en vertu de l'article 314*bis* du Code pénal.

b. Article 124 de la loi relative aux communications électroniques

36. L'article 124 de la loi *relative aux communications électroniques* du 13 juin 2005[10] (ci-après la "loi relative aux communications électroniques") dispose que "*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** ;*
- *identifier **intentionnellement** les personnes concernées par la transmission de l'information et son contenu ;*
- *(…) prendre connaissance **intentionnellement** de données en matière de communications électroniques et relatives à une autre personne ;*
- *modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues **intentionnellement ou non**.*"

37. Cette disposition concerne la prise de connaissance de *l'existence* de la communication électronique.

38. Tous ces actes peuvent être sanctionnés pénalement d'une amende de 50 à 50.000 euros (article 145 de la loi relative aux communications électroniques).

39. Il est important que la modification, la suppression, la divulgation, le stockage ou l'usage d'une manière quelconque de l'information, de l'identification ou des données soit punissable, sans qu'il ne soit question de la moindre intention.

40. Dans son arrêt du 1er octobre 2009, la Cour de cassation a encore répété que la prise de connaissance intentionnelle de l'existence d'un courrier électronique, ainsi que l'utilisation de cette connaissance ou des informations qui avaient été ainsi obtenues, intentionnellement ou non, étaient exclues pour toute personne n'ayant pas obtenu au préalable les consentements nécessaires (art. 124, 1° et 4° de la loi relative aux communications électroniques)[11].

41. Plus important encore, la Cour a décidé que la prise de connaissance du contenu d'un courrier électronique allait de pair avec la prise de connaissance et l'utilisation de celui-ci. Dans la doctrine, on a avancé que l'article 124 de la loi relative aux communications électroniques ne concernait pas la prise de connaissance du contenu d'un courrier électronique. Cet acte pourrait uniquement être sanctionné via l'article 314*bis* du Code pénal. Étant donné que cette dernière disposition pénale ne concernerait que la

[10] *M.B.* du 20 juin 2005.
[11] Cass., 1er octobre 2009, RG C.08.0064.N.

prise de connaissance d'un courrier électronique *pendant la transmission du message* et qu'une intention était requise, on partait du principe qu'en cas de prise de connaissance du contenu d'un courrier électronique par l'employeur, il n'y avait pas infraction à l'article 314*bis* du Code pénal. On pourrait déduire de l'arrêt de la Cour de cassation du 1er octobre 2009 (qui ne concernait pas une affaire relative au droit du travail) qu'un employeur qui utilise un courrier électronique (par exemple, dans le cadre d'un licenciement pour motif impérieux) est punissable, même lorsqu'il prend fortuitement connaissance de ce courrier électronique.

c. Exceptions à l'interdiction légale

42. Le droit au respect de la vie privée n'est pas absolu[12] et la situation particulière du rapport hiérarchique entre l'employeur et le travailleur doit être prise en considération[13].

43. En outre, le travailleur ne peut pas invoquer sa vie privée uniquement pour échapper aux conséquences de son comportement frauduleux[14].

44. DE CORTE affirme également qu' "*un individu ne peut invoquer la protection juridique résultant de la réglementation vie privée que dans les circonstances où il se prévaut effectivement de l'autoréalisation considérée comme digne de protection par le droit*". [traduction libre réalisée par le secrétariat de la Commission, en l'absence d'une traduction officielle] Selon DE CORTE, le juge doit veiller à ce que le droit au respect de la vie privée soit exercé dans le cadre de la 'finalité de la norme' du système juridique. La vie privée ne peut pas être utilisée pour échapper aux conséquences de délits commis ou d'un comportement illégitime[15]. Le droit à la protection de la vie privée est un droit fonctionnel.

45. HENDRICKX mentionne également *"le principe selon lequel on ne peut pas abuser de son droit au respect de la vie privée pour porter préjudice à un autre citoyen, sous peine de perdre son droit légitime à la protection"* [traduction libre réalisée par le secrétariat de la Commission, en l'absence d'une traduction officielle][16]. En d'autres termes, il faut essayer de concilier ces deux droits. L'article 8 de la CEDH laisse la marge nécessaire pour ce faire. La législation belge permet aussi que ces deux droits soient conciliés.

46. Toutefois, il va de soi que les attentes en matière de vie privée des travailleurs sont moins grandes sur le lieu de travail. Les attentes en matière de vie privée peuvent donc être définies comme étant les attentes qu'une personne a raisonnablement concernant le degré d'ingérence dans sa vie privée[17]. Les attentes en matière de vie privée du travailleur concernant les données dont il indique lui-même qu'il ne les considère pas comme des informations personnelles sont clairement moins grandes.

---

[12] Voir notamment Cass., 7 octobre 1981, *Arr. Cass.* 1981-82, 1983 ; Cass., 27 février 2001, *R.W.* 2001-2002, 1171.
[13] Cass., 27 février 2001, *A.J.T.* 2000-01, 949, note I. VERHELST.
[14] Voir par exemple C.T. Bruxelles, 22 juin 2000, *Computerrecht* 2001, 311.
[15] R. DE CORTE, "De achterkant van de privacy – Kan het beroep op privacy leiden tot straffeloos-heid?", *NJW.*, p. 808.
[16] F. HENDRICKX, *Privacy en arbeidsrecht*, n° 1 de la Bijzondere reeks ICA, Bruges, die Keure, 1999, 200.
[17] Voir F. HEYNDRICKX, *Privacy en arbeidsrecht*, Bruges, die Keure, 1999, 51.

47. Les paragraphes suivants traitent conjointement ces exceptions.

1° Le consentement de toutes les personnes impliquées dans la communication électronique

48. Il n'y a pas de violation de l'article 314*bis* du Code pénal ni de l'article 124 de la loi relative aux communications électroniques lorsque l'employeur obtient le consentement de tous les participants à la communication électronique à la prise de connaissance.

49. En ce qui concerne l'utilisation d'Internet, il pourrait suffire, le cas échéant, d'obtenir le consentement des travailleurs. Toutefois, la doctrine est divisée quant à la question de savoir dans quelle mesure le travailleur peut donner un tel consentement. Pour certains auteurs, il suffit de reprendre une disposition générale à cet égard dans le règlement de travail, dans le contrat de travail ou dans une politique relative à la messagerie électronique et à Internet. D'autres affirment, en référence aux travaux parlementaires, que le travailleur doit systématiquement donner à nouveau son consentement. Celui-ci pourrait être obtenu en faisant apparaître, dès le lancement du navigateur Internet, une fenêtre de texte invitant le travailleur à cliquer sur "ok" pour continuer.

50. Quant au contrôle de l'utilisation de la messagerie électronique, l'obtention du consentement peut constituer un problème pratique étant donné que toutes les parties impliquées dans la communication doivent donner leur consentement. Il est évident qu'il est difficile d'obtenir le consentement de participants qui ne sont pas des travailleurs de l'entreprise.

51. Dans le cadre d'un contrat de travail, il n'y a pas d'équilibre entre les parties en présence (si bien que la loi compense d'ailleurs ce déséquilibre par une multitude de mesures protectionnelles au bénéfice du travailleur), de sorte que le consentement du travailleur peut difficilement être considéré comme "libre" au sens où il est requis par la loi.

52. Il convient pourtant de constater que dans la jurisprudence, une certaine importance est quand même accordée à l'existence d'un consentement valable du travailleur. Ainsi, le Tribunal du travail de Bruxelles a décidé que les courriers électroniques découverts ne pouvaient pas être utilisés dans le cadre d'une procédure concernant le licenciement pour motif impérieux d'un travailleur. L'employeur ne pouvait en effet pas prouver qu'il avait obtenu le consentement du travailleur à la prise de connaissance de ces courriers électroniques et que la prise de connaissance avait eu lieu par inadvertance[18].

2° Exceptions techniques

53. L'article 125, 2° de la loi relative aux communications électroniques autorise les actes visés à l'article 124 lorsqu'ils 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.

[18] Trib. trav. Bruxelles, 4 décembre 2007, *J.T.T.* 2008, n° 1005, 179.

54. Certains auteurs ont interprété l'exception dont question comme permettant des interventions nécessitées sur le réseau de l'entreprise[19].

55. L'article 128 de la loi relative aux communications électroniques autorise les actes suivants (moyennant le respect de la loi vie privée) :

- l'enregistrement d'une communication électronique et des données relatives au trafic qui s'y rapportent réalisée dans les transactions commerciales licites comme preuve d'une transaction commerciale ou d'une autre communication professionnelle, à condition 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, avant l'enregistrement (les données sont effacées au plus tard à la fin de la période pendant laquelle la transaction peut être contestée en justice) ;

- 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 centers, à condition 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 (les données peuvent être conservées maximum un mois).

56. Ces deux dernières exceptions semblent ne pas offrir suffisamment de possibilités à l'employeur pour légitimer un contrôle général de l'utilisation de la messagerie électronique et d'Internet.

3° Autorisation légale

57. L'article 125, 1° de la loi relative aux communications électroniques prévoit que l'interdiction ne s'applique pas non plus "*lorsque la loi permet ou impose l'accomplissement des actes visés*" à l'article 124.

58. La question qui se pose est de savoir si les dispositions de la loi *relative aux contrats de travail* du 3 juillet 1978 constituent une base légale suffisante à cet effet. Le travail d'un travailleur est exécuté dans le cadre d'un contrat de travail ou dans une situation similaire mais sous une autorité. Une autorité implique la possibilité de diriger et de surveiller le travailleur (articles 2, 3, 4 et 5 de la loi relative aux contrats de travail). C'est dans le cadre de cette compétence de direction et de surveillance que s'inscrit le droit de contrôle de l'employeur. Bien entendu, cela s'applique également aux agents qui travaillent sous autorité, en vertu d'un statut.

[19] O. RIJCKAERT, "Surveillance des travailleurs : nouveaux procédés, multiples contraintes", *Orientations*, 2005, n°35, p. 51-52 ; 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.

59. L'article 16 de la loi relative aux contrats de travail stipule par ailleurs que l'employeur et le travailleur se doivent le respect et des égards mutuels et qu'ils sont *tenus d'assurer et d'observer le respect* des convenances et *des bonnes mœurs* pendant l'exécution du contrat.

60. L'article 17 de la loi relative aux contrats de travail prévoit en outre que "*le travailleur a l'obligation*:

1° d'exécuter son travail avec soin, probité et conscience, au temps, au lieu et dans les conditions convenus ;
2° d'agir conformément aux ordres et aux instructions qui lui sont donnés par l'employeur, ses mandataires ou ses préposés, en vue de l'exécution du contrat ; (…)".

61. La jurisprudence semble d'avis que ces dispositions peuvent constituer l'exception légale requise[20].

62. De plus, il faut également tenir compte de la responsabilité de l'employeur vis-à-vis de tiers. À cet égard, l'article 1384, troisième alinéa du Code civil stipule ce qui suit :

> *"On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde.*
> *(…)*
> *Les maîtres et les commettants, du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés. (…)".*

63. L'exigence selon laquelle il doit s'agir d'un dommage causé dans les fonctions auxquelles les préposés sont employés est interprétée au sens large par la jurisprudence. Il suffit que le fait qui a causé le dommage ait été commis pendant l'exercice de la fonction et qu'il ait un lien avec celle-ci, même si ce lien est indirect et occasionnel[21]. Le fait que le préposé a agi sur le lieu de travail et pendant les heures normales de service est considéré comme déterminant[22]. Cette large interprétation a pour conséquence

[20] Ainsi, la Cour du travail de Mons a déjà décidé dans un arrêt du 25 novembre 2009 (RDTI 2010, 81, note K. ROSIER) que les articles 16 et 17 de la loi relative aux contrats de travail étaient bien des dispositions légales qui, au sens de l'article 109*ter*E, § 1, 1 de la loi du 21 mars 1991 *portant réforme de certaines entreprises publiques économiques*, autorisent la prise de connaissance de données de connexions Internet d'un travailleur. La Cour du travail a en outre attiré l'attention sur le risque de propagation d'un virus dans un système informatique de l'employeur. La Cour du travail de Gand a également décidé que l'employeur était autorisé à procéder à un contrôle en vertu des dispositions de la loi relative aux contrats de travail qui obligent le travailleur à observer le respect des convenances et des bonnes mœurs pendant l'exécution du contrat (article 16), à exécuter son travail avec soin, probité et conscience, au temps, au lieu et dans les conditions convenus (article 17, 1°) et à agir conformément aux ordres et aux instructions qui lui sont donnés par l'employeur (article 17, 2°) (C.T. Gand, 9 mai 2005, *Soc. Kron.* 2006, 158). Dans un jugement du 22 juin 2000, le Tribunal du travail de Bruxelles a estimé (*Computerr.* (NL) 2001, 311) qu'un employeur pouvait invoquer l'article 16 de la loi relative aux contrats de travail en tant qu'autorisation légale pour pouvoir utiliser un courrier électronique d'un travailleur. Le travailleur concerné, qui avait envoyé une image pornographique par courrier électronique à une collègue féminine, a dès lors pu être licencié pour motif impérieux, sur décision du tribunal, et le courrier électronique en question a pu être soumis.
[21] Voir notamment Cass. 24 décembre 1980, *R.W.* 1981-1982, 2739 ; Cass. 12 décembre 1960, *RGAR* 1962, n° 6874 ; Cass. 27 mars 1944, *Pas.* 1944, I, 275.
[22] Voir notamment H. VANDENBERGHE, M. VAN QUICKENBORNE et P. HAMELINK, "Overzicht van rechtspraak (1964-1978), *TPR* 1980, 1336.

que le commettant est également responsable en cas d'abus de la fonction[23] et le commettant est également tenu pour responsable du dommage causé par un délit du préposé[24].

64. Il importe de souligner qu'il s'agit ici d'une responsabilité objective, sans faute. Lorsqu'un travailleur cause un dommage à un tiers en abusant du système informatique, l'employeur peut donc être tenu pour responsable de ce dommage. Face à cela, un certain droit de contrôle de l'employeur doit exister.

3. La CCT n° 81 du 26 avril 2002

65. Les partenaires sociaux se sont également penchés sur la problématique et le 26 avril 2002, la *CCT n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau* a été conclue.

66. Vu la hiérarchie des sources de droit en droit social, il faut tenir compte du fait que la CCT ne peut pas porter préjudice aux lois et normes internationales supérieures. Le commentaire qui précède la CCT le mentionne également. Le but de la CCT n° 81 est dès lors de "*préciser les normes de droit existantes tout en offrant la souplesse requise pour coller au plus près aux réalités que vivent les employeurs, les travailleurs et/ou leurs représentants*".

67. Pour l'application de la CCT n° 81, 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*".

68. D'après le commentaire de la CCT n° 81, la CCT "*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*".

69. Par données de communication électroniques en réseau, on vise aussi, selon la Cour du travail de Bruxelles, les courriers électroniques enregistrés[25].

70. La CCT n° 81 ne concerne pas les règles d'accès aux et/ou d'utilisation des moyens de communication électroniques en réseau de l'entreprise, qui sont la prérogative de l'employeur. L'employeur est donc libre de limiter l'utilisation d'Internet et de la messagerie électronique de ses travailleurs. Cela dépend de l'exercice de son autorité et de son droit de propriété.

---

[23] L. CORNELIS, *Beginselen van het Belgisch buitencontractuele aansprakelijkheidsrecht*, Anvers, Maklu, 1989, 231-232 ; A. VAN OEVELEN, "De civielrechtelijke aansprakelijkheid van de werknemer en de werkgever voor onrechtmatige daden van de werknemer in het raam van de uitvoering van de arbeidsovereenkomst", *R.W.* 1987-1988, 1202.
[24] Voir Cass. 9 février 1982, *Arr. Cass.* 1981-1982, 741.
[25] C.T. Bruxelles, 13 septembre 2005, *Computerr. (Ned.)* 2006, n° 2, 100.

71. Bien que l'employeur puisse donc par exemple bloquer l'accès à certains sites Internet, il faut toutefois, à la lumière de la jurisprudence précitée de la Cour européenne des droits de l'homme, se poser la question de savoir si tout usage privé peut être interdit. En outre, même le fait que l'employeur interdise tout usage personnel des moyens de communication en réseau ne peut pas constituer un sauf-conduit pour accéder aux données de communication du travailleur concerné. Dans un arrêt antérieur à la création de la CCT n° 81, la Cour du travail de Gand confirmait ce principe.

72. En vertu de la loi relative aux contrats de travail, l'employeur a le droit d'imposer, sans le moindre consensus ou la moindre participation des travailleurs, des directives et des obligations unilatérales concernant l'utilisation de l'informatique[26].

73. Le contrôle global des données de communication électroniques en réseau n'est autorisé par la CCT n° 81 que pour autant que les principes suivants soient respectés :

- le principe de finalité ;
- le principe de proportionnalité ;
- le principe de transparence.

a. Finalités du contrôle (principe de finalité)

74. L'employeur ne peut contrôler l'utilisation de la messagerie électronique et d'Internet que s'il poursuit l'une ou plusieurs des finalités ci-après, lesquelles doivent être définies de façon claire et explicite :

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

La Cour du travail d'Anvers a interprété cette disposition de façon restrictive. Selon la Cour du travail, il devait s'agir de *la consultation* des sites visés, ce qui suppose clairement une participation active de l'utilisateur, consistant à poser des actes destinés à visiter et à consulter de tels sites. La réception de courriers électroniques envoyés par autrui n'est pas considérée par la Cour du travail comme un acte pouvant être imputé ou reproché en tant que tel au destinataire de ces courriers électroniques et ne permet par conséquent pas à l'employeur d'effectuer un contrôle[27] ;

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 ;

[26] C.T. Gand (Sect. Bruges), 4 avril 2001, *J.T.T.* 2002, 49.
[27] C.T. Anvers (Sect. Hasselt), 15 novembre 2005, *Soc. Kron.* 2006, 153.

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

La Cour du travail de Liège a estimé que *l'employeur qui découvre par hasard dans la messagerie interne de l'entreprise un échange de mails entre deux travailleurs ayant accès à son système, qui évoque la possibilité d'introduire un virus dans ledit système est en droit d'accéder à la messagerie de ces travailleurs afin de procéder à un contrôle des données échangées entre eux*[28]. Dans sa position, la Cour du travail semble toutefois perdre de vue que la CCT n° 81 porte uniquement sur le contrôle des données de communication électronique en réseau et pas sur leur contenu.

b. Information (principe de transparence)

75. L'employeur qui entend installer un système de contrôle doit informer le conseil d'entreprise (ou, à défaut, le comité de prévention ou, à défaut, la représentation syndicale ou, à défaut, les travailleurs) de tous les aspects de ce contrôle, et ce préalablement à l'installation du système de contrôle. Ces informations doivent porter sur :

- la politique de contrôle ainsi que sur les prérogatives de l'employeur et du personnel de surveillance ;
- la ou les finalité(s) poursuivie(s) ;
- le fait que des données personnelles soient ou non conservées, le lieu et la durée de la conservation ;
- le caractère permanent ou non du contrôle.

76. Lors de l'installation d'un système de contrôle, l'employeur doit en outre informer les travailleurs individuels de tous les aspects du contrôle. Les informations doivent se rapporter aux éléments susmentionnés des informations collectives ainsi qu'aux aspects suivants :

- l'utilisation des outils mis à la disposition du travailleur pour l'exécution de son travail, y compris les restrictions relatives à l'utilisation dans le cadre de la fonction ;
- les droits, devoirs et obligations des travailleurs ainsi que les interdictions éventuelles en ce qui concerne l'utilisation des moyens de communication électronique en réseau de l'entreprise ;
- les sanctions prévues dans le règlement de travail en cas de non-respect des règles.

77. L'employeur peut choisir lui-même quels moyens utiliser pour informer les travailleurs : des instructions générales (circulaires, affichage, …), le règlement de travail, le contrat individuel de travail, des instructions lors de l'utilisation (mention sur écran de messages à l'allumage du poste de travail et/ou lors de l'activation de certains programmes). Selon la CCT n° 81, ces informations ne doivent

[28] C.T. Liège, 20 mars 2006, *R.R.D.* 2006, n° 118, 89, note K. ROSIER et S. GILSON.

donc pas obligatoirement être reprises dans le règlement de travail. C'est uniquement le cas si le contrôle est effectué en vue de mesurer le travail ou s'il concerne les compétences du personnel de surveillance ou si des sanctions disciplinaires sont infligées. Compte tenu de la participation dont jouissent les travailleurs dans l'élaboration et l'adaptation du règlement de travail, un règlement de travail offre le plus grand nombre de garanties. Le cas échéant, on peut opter pour une possibilité analogue pour les travailleurs afin de communiquer leurs remarques dans un registre.

c. Légitimité

78. Le traitement de données à caractère personnel est uniquement autorisé dans des cas bien déterminés, notamment lorsque la personne concernée a indubitablement donné son consentement, lorsque le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou lorsque le traitement est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée.

d. Évaluation

79. Les systèmes de contrôle installés doivent être régulièrement évalués en vue de propositions visant à les adapter aux progrès technologiques. Cette évaluation s'effectue au sein du conseil d'entreprise (à défaut de conseil d'entreprise, ces informations sont communiquées au comité de prévention, ou à défaut, à la représentation syndicale, ou à défaut, aux travailleurs). L'objectif de cette évaluation est d'examiner la possibilité de mieux réaliser la finalité de non-ingérence ou d'ingérence minimale dans la vie privée des travailleurs.

e. Contrôle (principe de proportionnalité)

80. Le contrôle des données de communication électroniques en réseau ne peut entraîner aucune ingérence dans la vie privée des travailleurs. Si le contrôle engendrait une telle ingérence, celle-ci devrait être limitée à un minimum (principe de proportionnalité).

81. Le commentaire de la CCT n° 81 précise que seules les données de communication électroniques en réseau nécessaires au contrôle peuvent être traitées et collectées, autrement dit les données qui, vu la finalité du contrôle, entraînent une ingérence aussi faible que possible dans la vie privée des travailleurs.

82. Dans cette phase, il est uniquement permis de collecter des données globales et l'identification des travailleurs individuels n'est pas autorisée :

- Internet : l'employeur peut collecter des données concernant la durée de la connexion par poste de travail mais ne peut pas individualiser les sites visités ;
- courrier électronique : l'employeur peut collecter des données concernant le nombre de messages envoyés par poste de travail ainsi que leur volume mais ne peut pas identifier le travailleur qui les a envoyés.

83. La CCT n° 81 ne précise pas les modalités d'un tel contrôle global sans individualisation des travailleurs. Une interprétation possible est que dans un premier temps, sur la base des informations se trouvant sur le serveur, des listes de données globales peuvent être constituées, listes ne permettant pas d'identifier des travailleurs individuels. Si, sur la base de ces listes générales, des anomalies sont soupçonnées, on peut procéder à l'identification des travailleurs individuels sur la base des autres données collectées et qui se trouvent sur le serveur (voir le point suivant relatif à la procédure d'individualisation).

f. Individualisation des données de communication électroniques en réseau

84. La CCT n° 81 contient des règles spécifiques en matière d'individualisation, à savoir *"l'opération consistant à traiter des données de communication électroniques en réseau collectées lors d'un contrôle installé par l'employeur en vue de les attribuer à un travailleur identifié ou identifiable"*.

85. L'individualisation doit s'effectuer de bonne foi et conformément à la finalité poursuivie par le contrôle. Seules les données qui sont nécessaires pour la finalité poursuivie par le contrôle peuvent être individualisées. Elles doivent être adéquates, pertinentes et non excessives au regard de cette finalité.

86. En fonction des finalités poursuivies par l'employeur, l'individualisation s'opérera dans le cadre d'une procédure directe ou indirecte.

g. Procédure directe

87. Une individualisation directe est autorisée lorsque l'employeur poursuit l'une ou plusieurs des finalités 1°-3° mentionnées au point 74.

88. L'employeur qui, dans le cadre de la poursuite de l'une de ces finalités, constate une anomalie à la lumière des données générales dont il dispose peut procéder directement à l'individualisation.

89. Des anomalies éventuelles peuvent par exemple être constatées par la consultation régulière des statistiques ou par l'utilisation de toute autre source d'information.

h. Procédure indirecte

90. Si l'employeur poursuit la finalité visée au point 4° du point 74 du présent document, une procédure spécifique doit être suivie avant de pouvoir procéder à l'individualisation.

91. Dans un premier temps, l'employeur doit respecter une phase préalable d'information, laquelle a pour objet de porter à la connaissance du ou des travailleurs, de manière certaine et compréhensible, l'existence de l'anomalie et de les avertir d'une individualisation des données de communication électroniques en réseau lorsqu'une nouvelle anomalie de même nature sera constatée. La communication de cette information par l'employeur doit revêtir un caractère de rappel ou de mise au point des principes

et règles fixés dans l'entreprise de manière à éviter la survenance d'une nouvelle anomalie de même nature.

92. Lorsque par la suite, un travailleur individuel est tenu pour responsable d'une (nouvelle) anomalie, il doit être invité à un entretien personnel par l'employeur. Cet entretien doit avoir lieu avant toute décision ou évaluation relative au travailleur. Il a pour but de permettre au travailleur de faire part à l'employeur de ses objections vis-à-vis de la décision ou de l'évaluation envisagée et de s'expliquer sur l'utilisation faite des moyens de communication électroniques en réseau mis à sa disposition.

4. Article 550*bis* du Code pénal

93. L'article 550*bis*, § 1, du Code pénal punit d'un emprisonnement de 3 mois à 1 an et d'une amende de 26 euros à 5.500 euros (hors centimes additionnels) quiconque *"sachant qu'il n'y est pas autorisé, accède à un système informatique ou s'y maintient"*. S'il est question d'intention frauduleuse, la peine d'emprisonnement est de 6 mois à 2 ans.

94. Ces dispositions s'appliquent pour le piratage du système informatique depuis l'extérieur. Dans le cadre d'un contrôle par l'employeur, ce ne sera généralement pas le cas.

95. Pour le fait d'accéder "en interne" à un système informatique avec une intention frauduleuse ou dans le but de nuire en outrepassant son pouvoir d'accès à un système informatique, l'article 550*bis*, § 2 du Code pénal prévoit un emprisonnement de six mois à deux ans et une amende de vingt-six euros à vingt-cinq mille euros.

96. Celui qui se trouve dans une de ces situations et qui :

> *" 1° soit reprend, de quelque manière que ce soit, les données stockées, traitées ou transmises par le système informatique ;*
> *2° soit fait un usage quelconque d'un système informatique appartenant à un tiers ou se sert du système informatique pour accéder au système informatique d'un tiers ;*
> *3° soit cause un dommage quelconque, même non intentionnellement, au système informatique ou aux données qui sont stockées traitées ou transmises par ce système ou au système informatique d'un tiers ou aux données qui sont stockées, traitées ou transmises par ce système ; est* [également] *puni (d'un emprisonnement de un à trois ans et d'une amende de vingt-six euros à cinquante mille euros"*

97. La question de savoir si la prise de connaissance d'une communication électronique par l'employeur est punissable en vertu de l'article 550*bis* du Code pénal dépendra donc de la question de savoir si l'employeur a outrepassé son pouvoir d'accès. La réponse à cette question devra être apportée à l'aide de l'autre législation examinée.

98. En outre, une incrimination requiert également l'existence d'une intention frauduleuse.

5. La protection des données à caractère personnel : la LVP

99. La Commission entend rappeler très fermement l'application de la loi du 8 décembre 1992 dont les dispositions impératives s'imposent aux responsables de traitements, en l'occurrence l'ensemble des employeurs, que leurs activités relèvent du secteur public ou du secteur privé : obligations de forme, de procédure, objectifs à atteindre. Ces obligations ne peuvent être contournées ou écartées. Aucun argument porté à la connaissance de la Commission ne permet de considérer que ces obligations constitueraient des charges telles qu'elles feraient obstacle au développement de l'activité économique ou à l'action de l'administration publique.

100. La LVP est une législation transversale qui a pour vocation à s'appliquer y compris dans le cadre des relations de travail. La LVP définit les conditions dans lesquelles un responsable de traitement peut traiter des données à caractère personnel.

101. L'article 1, § 1, de la LVP définit les données à caractère personnel comme étant "*toute information concernant une personne physique identifiée ou identifiable, désignée ci-après "personne concernée*" tout en précisant qu' "*est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale*".

102. La LVP vise donc la protection de toutes les données à caractère personnel, quel que soit leur degré de sensibilité et qu'elles aient ou non un rapport avec la vie privée de l'intéressé. Vu sous cet angle, les données relatives à un travailleur bénéficient, également sur le lieu de travail, d'une protection par la LVP. Les adresses de messagerie électronique professionnelles personnalisées, les données de communication électroniques (qu'il s'agisse de messages électroniques ou de connexions Internet, que ces communications soient de nature professionnelle ou non), le contenu des messages électroniques envoyés ou reçus à une telle adresse (qu'ils revêtent ou non un caractère professionnel), sont des données à caractère personnel dès lors qu'elles concerneront une personne identifiée ou identifiable.

103. La LVP s'applique à tout traitement de données à caractère personnel automatisé en tout ou en partie, ainsi qu'à tout traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. Par "traitement", on entend "*toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction de données à caractère personnel*" (article 1, § 2 LVP).

104. Ainsi, le contrôle ou la prise de connaissance licite d'informations générées par les outils informatiques ou de communication électronique utilisés par le travailleur dans le cadre de la relation de travail supposent généralement un traitement de données à caractère personnel. (passage en double!)

105. À l'occasion de telles opérations, les dispositions de la LVP doivent donc être respectées et doivent encadrer les démarches des différents responsables et intervenants, qu'il s'agisse d'éviter que des données à caractère personnel ne soient exploitées illicitement, de manière abusive et sous le couvert d'une apparente automaticité, en marge d'une intervention poursuivant d'autres fins, ou qu'il s'agisse de garantir que le traitement *a priori* licite et légitime de telles données ne porte pas atteinte aux libertés et droits fondamentaux des personnes concernées.

106. La LVP met à charge des responsables de traitements de données à caractère personnel une série d'obligations, sous forme d'objectifs à atteindre, tout en leur reconnaissant une liberté, une autonomie et donc une responsabilité quant aux mesures à prendre pour exécuter leurs obligations et quant à la matérialité des éléments pertinents permettant de justifier leurs décisions.

107. Tout traitement de données doit ainsi poursuivre **une ou plusieurs finalités spécifiques et déterminées** dès la mise en place du traitement. La LVP interdit la réutilisation de données pour des finalités qui ne sont pas compatibles avec ces finalités d'origine, sauf exceptions prévues par la loi[29].

108. À titre d'exemples recueillis dans la pratique concernant les objectifs que pourrait poursuivre l'employeur qui souhaiterait conserver, accéder à ou prendre connaissance de communications électroniques ou de données de communications électroniques, il pourrait s'agir d'assurer une continuité des services prestés en cas d'absence, de décès du travailleur ou de départ de celui-ci de l'entreprise, de conserver des documents à des fins de preuve, ou encore un contrôle. En ce qui concerne les opérations de contrôle, on peut se référer aux objectifs retenus à l'article 5 de la CCT n° 81.

109. Ces **finalités** doivent en outre être **légitimes**. L'article 5 de la LVP prévoit six cas de figure dans lesquels la finalité est *a priori* légitime et le responsable du traitement doit pouvoir justifier que le traitement de données s'inscrit dans au moins un de ces six cas de figure limitativement énumérés.

110. À cet égard, la Commission estime qu'un traitement de données réalisé à l'occasion d'une opération de contrôle de travailleurs pourrait, le cas échéant, trouver son fondement dans l'exécution des contrats de travail, vu la nature de ce contrat (article 5, b) de la LVP) ou dans l'exécution d'une obligation similaire imposée en vertu de la loi pour les employeurs relevant du secteur public (article 5, c) de la LVP). Complémentairement, il faut considérer la possibilité que ce traitement de données soit nécessaire à la poursuite d'un intérêt légitime de l'employeur (article 5, f) de la LVP).

111. La Commission estime par contre que le consentement du ou des travailleurs concernés ne peut constituer la base légale autorisant le contrôle patronal des actes numériques accomplis dans le cadre de la relation de travail ou à l'aide des outils de travail. En raison des rapports de force existant entre les parties, un consentement individuel des travailleurs concernés ne pourrait être considéré comme véritablement libre.

112. Dans les conditions qui sont celles d'un contrat de travail, le consentement du travailleur ne peut pas être considéré comme "libre" au sens où il est requis par la LVP. En effet, si le droit du travail

[29] Article 4, § 1, 2° de la LVP.

consacre par des termes clairs l'autorité de l'employeur et la subordination du travailleur, il affirme aussi le déséquilibre entre les deux parties au contrat, au point de compenser ce déséquilibre par une multitude de dispositions protectionnelles au bénéfice du travailleur.

113. L'arrêté royal de 2001 a d'ailleurs tiré les conséquences de cette situation particulière, en spécifiant : "*Lorsque le traitement de données à caractère personnel visées aux articles 6 et 7 de la loi est exclusivement autorisé par le consentement écrit de la personne concernée, ce traitement est néanmoins interdit lorsque le responsable du traitement est l'employeur présent ou potentiel de la personne concernée ou lorsque la personne concernée se trouve dans une situation de dépendance vis-à-vis du responsable du traitement, qui l'empêche de refuser librement son consentement. Cette interdiction est levée lorsque le traitement vise l'octroi d'un avantage à la personne concernée*"[30].

114. Dans le même sens, le Groupe 29 a conclu que : "*Si un employeur doit traiter des données à caractère personnel comme conséquence inévitable et nécessaire de la relation professionnelle, il fait fausse route s'il essaie de légitimer ce traitement par le consentement. L'on peut recourir au consentement s'il s'applique strictement au cas où le travailleur est complètement libre de le donner et a la possibilité d'y renoncer par la suite sans préjudice.*"[31].

115. Le traitement doit également être **proportionné**. Il ne suffit pas que la surveillance puisse être motivée par l'exécution du contrat de travail ou de la tâche administrative (p. ex. surveiller le respect des instructions par le travailleur) et éventuellement, en outre, par la réalisation de l'intérêt légitime poursuivi par l'employeur (p. ex. monitorer le fonctionnement ou les performances de l'entreprise), encore faut-il que l'objectif spécifique poursuivi à cette occasion réponde aux besoins ou aux règles de l'entreprise ou découle de la nature du contrat de travail ou de la tâche à exécuter, et que le traitement mis en œuvre s'avère nécessaire pour atteindre cet objectif.

116. Par ailleurs, les données traitées à cette occasion doivent également être adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement. Leur durée de conservation ne peut excéder celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement (article 4, § 1er, 5° de la LVP).

117. Le responsable de traitement doit également s'assurer que les données traitées sont exactes et si nécessaire mises à jour (article 4, § 1er, 4° de la LVP).

118. L'article 12*bis* de la LVP interdit qu'une décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative soit prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité. Si cette interdiction ne

[30] Arrêté royal du 13 février 2001 *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*.
[31] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48fr_sum.pdf. Il s'agit d'un résumé de l'avis du Groupe de travail "article 29" *sur le traitement des données à caractère personnel dans le contexte professionnel*. Le Groupe 29 est l'instance européenne qui réunit les autorités de contrôle et de protection des données à caractère personnel de tous les pays membres de l'Union européenne.

s'applique pas lorsque la décision est prise dans le cadre d'un contrat ou est fondée sur une disposition prévue par ou en vertu d'une loi, d'un décret ou d'une ordonnance, il est exigé que ce contrat ou cette disposition contienne des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de l'intéressé. Ainsi, il devra au moins être permis à la personne concernée de faire valoir utilement son point de vue.

119. Enfin l'article 4, § 1, 1° de la LVP impose un principe de loyauté dans la mise en œuvre d'un traitement de données à caractère personnel. Une application de ce principe se retrouve d'ailleurs dans l'exigence de **transparence** imposée au responsable de traitement et qui se traduit par l'obligation de fournir certaines informations aux travailleurs concernés notamment sur la finalité de traitement et de déclarer le traitement préalablement à la Commission[32]. S'il existe des exceptions à ces deux obligations, la Commission estime qu'elles ne sont *a priori* pas applicables en l'espèce[33].

120. Par ailleurs, le responsable des traitements réalisés à l'occasion d'un contrôle ou d'une surveillance, devra en outre prendre toutes les mesures permettant de s'assurer que les **droits des travailleurs concernés sont respectés ou peuvent être exercés**[34] et que la **sécurité du traitement est assurée**[35], notamment en cas de sous-traitance de certaines opérations de traitement, afin notamment d'empêcher une exploitation ultérieure illicite des informations recueillies. Ces obligations impliquent notamment que le responsable du traitement veille à ce que, pour les personnes agissant sous son autorité, l'accès aux données et les possibilités de traitement soient limités à ce dont ces personnes ont besoin pour l'exercice de leurs fonctions ou à ce qui est nécessaire pour les nécessités du service (article 16, § 2, 2°) et qu'il informe les personnes agissant sous son autorité des dispositions de la présente loi et de ses arrêtés d'exécution, ainsi que de toute prescription pertinente, relative à la protection de la vie privée à l'égard des traitements des données à caractère personnel (article 16, § 2, 3°).

121. Il devra également se conformer à toutes les autres obligations définies par la LVP.

II.3 CONCLUSION

122. Il est explicitement reconnu que les travailleurs ont également droit à la protection de leur vie privée au travail. Toutefois, la relation de travail a un impact important sur l'exercice des droits fondamentaux par le travailleur. Au travail, l'employeur exerce en effet une autorité, ce qui implique qu'il dirige et contrôle le travail de ses travailleurs. Au travail, les prévisions en matière de respect de la vie privée du travailleur sont dès lors moins grandes que lorsque le travailleur pose les mêmes actes dans le cercle familial.

123. Le droit d'autorité de l'employeur implique que ce dernier est libre d'autoriser ou d'interdire l'utilisation d'Internet et de la messagerie électronique au travail.

---

[32] Voy. à cet égard les articles 9 et 17 de la LVP.
[33] Voy. à cet égard les exceptions prévues à ces obligations respectivement aux articles 9, § 2, d'une part, et 17 de la LVP et 51 à 62 de l'arrêté royal du 13 février 2001, d'autre part.
[34] Il s'agit des droits d'accès, de rectification et d'opposition tels que décrits aux articles 10, 11 et 12 de la LVP.
[35] Voy. à cet égard les obligations décrites à l'article 16 de la LVP.

124. Les articles 2, 3, 4 et 5 de la loi relative aux contrats de travail prévoient, comme un élément essentiel du contrat, l'autorité de l'employeur (c'est-à-dire ses pouvoirs de direction et de surveillance).

125. L'article 16 de la loi relative aux contrats de travail prévoit également que les deux parties se doivent le respect et des égards mutuels. L'article 17 de cette même loi indique que le travailleur est obligé d'exécuter son travail avec soin, probité et conscience et d'agir conformément aux ordres et aux instructions de son employeur.

126. La Commission estime que ces dispositions, ainsi que les directives établies dans la CCT n° 81, sont suffisamment claires pour définir dans quelle mesure l'employeur dispose d'un quelconque droit de contrôle. Aux yeux de la Commission, ces dispositions impliquent une autorisation légale, ce qui exclut toute violation de l'article 124 de la loi relative aux communications électroniques, pour autant que l'employeur respecte les principes de finalité, de transparence et de proportionnalité, définis plus en détail ci-après.

127. Dans ce cas, il ne peut pas non plus être question d'intention frauduleuse, comme requis dans l'article 550*bis* du Code pénal. Il ne s'agit pas non plus d'une prise de connaissance du contenu d'un courrier électronique pendant sa transmission, comme requis pour être punissable en application de l'article 314*bis* du Code pénal.

128. La Commission estime que le consentement du (des) travailleur(s) concerné(s) ne peut pas constituer la base légale autorisant un contrôle patronal des actes numériques accomplis par les travailleurs dans le cadre de la relation de travail ou à l'aide des outils de travail. En raison des rapports de force existant entre les parties, un consentement individuel des travailleurs concernés ne pourrait être considéré comme véritablement libre.

129. La Commission énumère ci-après des principes auxquels l'employeur doit se conformer lors de l'exercice de son droit de contrôle.

Principe 1 : principe de finalité

130. Le principe de finalité implique tout d'abord que les finalités d'un accès à la communication électronique du travailleur ou d'un contrôle de cette communication doivent être légitimes.

131. Toute ingérence dans ce droit fondamental doit pouvoir s'appuyer sur une finalité légitime. Le contrôle doit être adéquat, pertinent et non excessif au regard de la finalité du traitement, si bien que les données à caractère personnel sélectionnées doivent être évaluées selon la finalité annoncée. Les finalités pour lesquelles un quelconque contrôle est effectué ne peuvent pas être définies de façon vague et imprécise. Il convient de déterminer clairement au préalable à quelles fins et selon quelles modalités le contrôle ainsi que les éventuelles données traitées pourront être/seront utilisés ultérieurement. Ceci n'empêche pas que les données obtenues puissent être utilisées pour une autre

finalité que celle annoncée, pour autant que cette utilisation ne soit pas inconciliable avec la finalité initiale.

132. Les données doivent toujours être traitées loyalement (le travailleur ne peut être pris "en traître"), que ce soit dans le cadre d'un contrôle ou dans un autre but, pour des finalités qui ne soient pas incompatibles avec les attentes raisonnables des travailleurs concernés. Le traitement de données doit donc se dérouler conformément à la ou aux finalités annoncées. Si le traitement s'effectue dans le cadre d'une autre finalité, celle-ci doit être compatible avec la finalité initiale et l'employeur doit prendre les mesures nécessaires pour éviter des erreurs d'interprétation sur le résultat de l'opération. Le fait que l'employeur conserve des données à des fins de preuve ou pour le besoin du suivi de ses activités ne suffit pas à justifier qu'un contrôle soit effectué sur ces données (les informations faisant l'objet d'une duplication sur un réseau, de sauvegardes et d'archivage – back-up – sont particulièrement concernées).

Principe 2 : principe de transparence

133. L'employeur doit clairement indiquer à ses travailleurs dans quelle mesure l'utilisation d'Internet et de la messagerie électronique est autorisée au sein de l'entreprise et de quelle façon l'accès à ces outils ou leur contrôle sera exercé.

Principe 3 : principe de proportionnalité

134. Toute restriction de la vie privée du travailleur doit être limitée autant que possible. Ce n'est qu'une fois que toutes les mesures préventives se sont avérées insuffisantes que l'employeur peut procéder à la constatation de l'existence d'un quelconque abus. En cas de contrôle impliquant une quelconque atteinte au droit au respect de la vie privée du travailleur, cette atteinte sera limitée autant que possible en suivant un plan par phases, tel que décrit dans la CCT n° 81. Ce n'est que si toutes ces opérations s'avèrent insuffisantes pour constater l'abus présumé que l'employeur peut prendre connaissance du contenu de la communication à laquelle le travailleur a pris part.

III. UTILISATION DE LA PREUVE (OBTENUE IRRÉGULIÈREMENT)

135. Dans l'arrêt dit "Antigone" du 14 octobre 2003, la Cour de cassation a estimé qu'une preuve obtenue irrégulièrement ne doit donner lieu à l'exclusion que si le respect de certaines exigences de forme est prescrit à peine de nullité, si l'irrégularité commise a entaché la fiabilité de la preuve ou si l'usage de la preuve est contraire au droit à un procès équitable[36]. Dans l'arrêt du 23 mars 2004, la Cour de cassation a réitéré cette position en ajoutant qu'*"il appartient au juge d'apprécier l'admissibilité d'une preuve obtenue illicitement à la lumière des articles 6 de la CEDH et 14 du PIDCP compte tenu des éléments de la cause prise dans son ensemble, y compris le mode d'obtention de la preuve et les circonstances dans lesquelles l'illicéité a été commise"*[37].

[36] Cass. 14 octobre 2003, RG P.03.0762.N, avec conclusions de M. l'avocat général DE SWAEF.
[37] Cass. 23 mars 2004, RG P.04.0012.N.

136. La Cour européenne des droits de l'homme a également déjà approuvé cette jurisprudence[38].

137. Dans l'arrêt "Chocolatier Manon" du 2 mars 2005, la Cour de cassation a accepté que le juge ait tenu compte d'images vidéo qu'un employeur avait obtenues en violation de la CCT 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 de travail*. La Cour considère que, vu que la méconnaissance par l'employeur de son obligation d'information prévue dans la CCT n° 68 n'est pas sanctionnée de nullité, il appartient au juge d'apprécier les conséquences de cette méconnaissance sur la recevabilité des moyens de preuve obtenus de façon irrégulière[39].

138. Dans son arrêt du 10 mars 2008[40], la Cour de cassation a accepté que ces mêmes règles d'exclusion de la preuve soient applicables en matière civile et sociale. Sauf si la loi prévoit expressément le contraire, le juge doit examiner l'admissibilité d'une preuve obtenue de façon irrégulière à la lumière des articles 6 de la CEDH et 14 du PIDCP en tenant compte de tous les éléments de la cause, y compris de la manière suivant laquelle la preuve a été recueillie et des circonstances dans lesquelles l'irrégularité a été commise. Ainsi, la Cour a décidé que sauf en cas de violation d'une formalité prescrite à peine de nullité, une telle preuve ne peut être écartée que si elle a été recueillie d'une manière qui est entachée d'un vice préjudiciable à sa crédibilité ou qui porte atteinte au droit à un procès équitable. Le juge qui procède à cette appréciation peut notamment tenir compte de l'une ou de plusieurs des circonstances suivantes :

- le caractère purement formel de l'irrégularité ;
- les conséquences sur le droit ou la liberté protégés par la règle transgressée ;
- la circonstance que l'irrégularité imputée à l'instance chargée de la détection, de l'investigation et des poursuites d'infractions est intentionnelle ou non ;
- la circonstance que la gravité de l'infraction dépasse de loin l'irrégularité commise ;
- le fait que la preuve recueillie de manière irrégulière concerne uniquement un élément matériel de l'existence de l'infraction ;
- le fait que l'irrégularité qui a précédé ou contribué à la constatation de l'infraction est hors de proportion avec la gravité de celle-ci.

139. Bien que l'affaire portait sur les conséquences d'une instruction sur une affaire civile (la suspension par l'ONEM), la Cour semble pourtant ainsi étendre l'application des principes de la jurisprudence Antigone rendue en droit pénal au droit civil/social.

140. Ces principes ont également déjà été bien accueillis par les juridictions du travail. Ainsi, dans son jugement du 1er septembre 2008[41], le Tribunal du travail de Gand a décidé que les courriers électroniques que le travailleur avait envoyés et qui ont permis le lancement d'une activité concurrente pouvaient quand même être utilisés pour accepter le licenciement pour motif impérieux bien que le contrôle n'avait

[38] Arrêt Lee Davies c. Belgique du 28 juillet 2009, www.echr.coe.int ; F. SCHUERMANS, "Antigoon-rechtspraak nu definitief in de fase van de rustige vastheid", *R.A.B.G.* 2010, 17-24.
[39] Cass. 2 mars 2005, *Arr. Cass.* 2005, n° 3, 506, concl. VANDERMEERSCH; *Rev.dr.pén.* 2005, n° 6, 668.
[40] *Pas.* 2008, n° 3, 652 ; *RCJB* 2009, n° 3, 325.
[41] TGR-TWVR 2009, n° 4, 275.

pas été annoncé. Le tribunal du travail a constaté qu'en dépit de cette illégitimité, la fiabilité de la preuve n'était pas entachée, il n'était pas porté atteinte au droit à un procès équitable et que dès lors, la preuve obtenue pouvait quand même être utilisée. La Cour du travail d'Anvers a également appliqué les mêmes principes dans son arrêt du 2 septembre 2008[42]. Depuis lors, plusieurs décisions ont fait application de la jurisprudence dans les litiges sociaux[43].

141. La Commission estime que le juge qui se trouve se trouve en dehors de ces hypothèses et face à un problème de cybersurveillance devrait faire un examen de mise en balance entre la faute commise et l'atteinte au droit à la vie privée (« la gravité de « l'infraction » qui a permis la constatation excède manifestement l'irrégularité commise »).

142. Si le travailleur a commis une atteinte à la loi, le fait de ne pas avoir respecté certaines règles procédurales relatives à la vie privée ne pourrait justifier en soi que les preuves soient écartées.

143. Si le travailleur n'a pas respecté les règles internes d'utilisation des technologies en réseau fixé par l'employeur, la Commission trouverait par contre injuste que ce dernier puisse présenter de manière fructueuse une preuve en justice s'il ne respecte pas lui-même ses propres obligations professionnelles, du fait de la loi ou de son propre règlement de travail (tel qu'informer ses travailleurs, prévoir des procédures de contrôle, les respecter, etc.).

[42] *Or.* 2008, n° 9, 261.
[43] Voy. notamment C.T. Liège (Sect. Namur), 14 décembre 2010, R.G. n°2009/AN/8.833; Trib. trav. Charleroi, (1ère ch.), 16 juin 2010, *Bull. Ass.*, 2010, n° 372, p. 294.