Recommandation n° 08/2012 du 2 mai 2012

Concerne : recommandation d'initiative relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail (CO-AR-2010-002)

La Commission de la protection de la vie privée (ci-après "la Commission") ;

Vu la loi du 8 décembre 1992 *relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* (ci-après "la LVP"), en particulier l'article 29 ;

Vu la consultation publique ;

Vu le rapport du Vice-Président ;

Émet, le 2 mai 2012, la recommandation suivante :

I. INTRODUCTION

I.1. CONTEXTE DE LA RECOMMANDATION

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. 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. Dans la présente recommandation, l'attention 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 qui 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.

4. 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 à l'Internet. 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 à titre privé 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).

5. Il convient toutefois de constater d'emblée que l'accès aux données de communication électroniques ou aux données d'Internet ne relève pas uniquement d'une question de surveillance – vérifier si le personnel n'exagère pas dans son utilisation de l'Internet et de la messagerie électronique de l'employeur à des fins privées – 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 de la correspondance électronique (archivage) mais également de permettre une continuité du service en cas d'absence, de départ ou de décès du travailleur (accéder aux courriers électroniques professionnels qu'un travailleur reçoit pendant son absence pour pouvoir continuer à assurer le bon fonctionnement de l'entreprise/de l'administration publique).

6. En effet, le travailleur, en exécution de son contrat de travail ou de son statut, 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.

7. 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 lui-même.

8. Quelle que soit la situation, la question demeure la même : le travailleur peut-il invoquer la LVP ou d'autres dispositions légales 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 ?

9. 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.

10. Cette complexité est due aux diverses normes légales qui trouvent à s'appliquer lorsqu'il s'agit de prendre connaissance de communications électroniques et de données de communication sur le lieu de travail.

I.2. CONTENU ET DESTINATAIRES DE LA RECOMMANDATION

11. La Commission souhaite informer les employeurs et les travailleurs, ainsi que 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 concernent la gestion et le contrôle de l'utilisation de l'outil informatique par les travailleurs.

12. Elle limitera sa réflexion aux communications électroniques que sont les courriers électroniques et les connexions Internet et ne se prononcera donc pas sur la problématique que représentent d'autres moyens de communication que la messagerie électronique et l'Internet, comme notamment les communications téléphoniques, les sms ou encore la géolocalisation[1].

13. La Commission est bien consciente que la portée de ce document (utilisation de la messagerie électronique et d'Internet via l'ordinateur du bureau mis à la disposition par l'employeur) peut être perçue comme restrictive. L'utilisation d'appareils portables par exemple apporte une dimension supplémentaire à la problématique du contrôle de l'employeur, parce que l'utilisation de tels appareils ne se limite pas alors aux murs de l'entreprise et/ou aux heures de bureau et soulève donc plus de questions, notamment en matière de protection des données professionnelles qui s'y trouvent. C'est a fortiori le cas si les appareils portables ne sont pas la propriété de l'employeur. En effet, cet élément qui peut également justifier le contrôle patronal (article 544 du code civil), est levé dans ce cas. Dans ce cas, il est de toute manière question d'usage mixte inhérent par le travailleur (tant à des fins professionnelles que privées). La Commission estime toutefois qu'elle doit limiter la portée de sa recommandation à ce qui a été abordé concrètement dans la consultation publique (voir le point 18). La Commission peut, le cas échéant, encore émettre des recommandations distinctes[2] sur ces autres questions.

14. Il sera fait référence aux communications elles-mêmes (à savoir le contenu d'un courrier électronique ou d'une page Internet 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).

15. La plupart des données générées par les outils de travail électroniques mis à disposition des travailleurs sont conservées, 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.

16. La Commission entend se pencher sur les conditions dans lesquelles ces données peuvent être ainsi conservées pour certaines finalités et les conditions dans lesquelles il peut y être accédé, que ce

[1] Concernant d'autres moyens de communication sur le lieu de travail, il existe d'ailleurs déjà plusieurs avis :
- géolocalisation via les véhicules de service : avis n° 12/2005 du 7 septembre 2005 ;
- enregistrement de conversations téléphoniques effectuées dans le cadre des services bancaires : recommandation n° 01/2002 du 22 août 2002 ;
- enregistrement des appels téléphoniques vers les commissariats de police et les hôpitaux ainsi qu'à partir de ceux-ci : recommandation n° 07/2011 du 21 décembre 2011 ;
- dans son avis n° 32/2011 du 30 novembre 2011, dans le cadre de l'utilisation du GSM (à des fins professionnelles et privées), la Commission recommande à l'employeur de prévoir deux options pour les travailleurs (la facturation scindée ou la déclaration sur l'honneur dans laquelle le travailleur s'engage à ne pas utiliser le GSM professionnel à des fins privées).

[2] Ainsi, une recommandation relative aux fleetloggers est en cours de préparation.

soit dans le cadre d'un contrôle ou d'une surveillance, ou d'une autre finalité. La Commission utilisera ci-après 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 de travail utilisé par un travailleur que sur d'autres supports sur lesquels les données sont sauvegardées (serveur, supports de sauvegarde, etc.).

17. La Commission rappellera les dispositions légales applicables. Elle entend, à l'occasion de la présente recommandation, réexaminer ses positions [3] adoptées précédemment en appréciant l'application de toutes les normes pertinentes, dont les dispositions contraignantes du droit du travail, à la lumière des dispositions de la LVP (cf. le point II) et elle évoquera également la question de la régularité de preuves recueillies au mépris des dispositions applicables (cf. le point III), vu la révolution jurisprudentielle qui s'est produite concernant ce concept. Elle formulera enfin, sous la forme de recommandations juridiques et techniques, une série de bonnes pratiques qui constituent des exemples ou des moyens de tenir compte de la LVP dans le cadre d'un accès patronal aux moyens de communication électroniques et qu'elle considère à même de prévenir les conflits entre les intérêts des employeurs et la protection des droits des travailleurs (voir le point IV).

I.3. PROCEDURE

18. La présente recommandation a été soumise au préalable à une consultation publique qui s'est déroulée entre le 15 juillet 2011 et le 30 novembre 2011 afin de permettre aux responsables de traitements 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

[3] La Commission s'est déjà 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 de la messagerie électronique et de l'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.*

surveillance et du contrôle des moyens de communication électroniques et informatiques dans le cadre de la relation de travail.

19. Les dizaines de réactions[4] qui ont été transmises en la matière ont en fait surtout révélé un besoin de précision de certains passages. De plus, il y avait un plaidoyer en faveur d'un élargissement du champ d'application des textes (autres formes de communication sur le lieu de travail et modalités de contrôle patronal de celles-ci, y compris le contrôle des travailleurs mobiles et même du télétravailleur, cf. le point 13). Bien que la Commission ne soit pas indifférente à cette remarque, en tenir compte impliquerait l'ajout de nouvelles thématiques qui n'ont pas fait l'objet de la procédure proprement dite de consultation publique. Le fait que la présente recommandation ne traite que de l'utilisation d'Internet et de la messagerie électronique au départ d'un ordinateur de l'employeur présente l'avantage que l'accent est mis sur les règles de base et les principes de la LVP qui s'appliqueront évidemment aussi à ces autres situations plus spécifiques. Les prescriptions de la LVP, qui donnent quoi qu'il en soit le ton dans la problématique de la cybersurveillance, offrent une solution appropriée et souple permettant le maintien ou le développement de certaines pratiques en rapport avec le contrôle et la prise de connaissance par l'employeur d'autres données de communication électroniques que les données d'Internet et les données de la messagerie électronique et sanctionnant en même temps des abus dans ce domaine.

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

[4] Ces réactions provenaient de divers milieux: la Fédération des Entreprises de Belgique, le groupe de travail du droit du travail de la CSC, le syndicat des employés CNE-NVK, les cabinets d'avocats Lydian et Claeys & Engels, le gouvernement flamand (e-government et administration ICT), la section POL (politique de sécurité de l'information) du groupe de travail GTSI, y compris des représentants des organismes publics de la Région Wallonne, de la Communauté française et de la Communauté germanophone (tels qu'ETNIC, FOREM, …), Beltug, LSEC, la police fédérale, la zone de police de Lebbeke - Buggenhout et Febetra. Ces réactions ont contribué au résultat final actuel.

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[5]. L'arrêt *Copland* contre le Royaume-Uni est intéressant[6]. 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

[5] 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.
[6] Copland c. Royaume-Uni, 3 avril 2007, à consulter sur http://www.echr.coe.int.

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[7].

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*[8] doit également être mentionnée. Cette directive a été transposée en Belgique (la LVP, telle que modifiée par la loi du 11 décembre 1998), de sorte qu'en tant que telle, cette directive ne fera l'objet d'aucun examen approfondi ci-après.

26. On peut également faire référence à un recueil de directives pratiques de l'Organisation Internationale du Travail (OIT) relatives à la protection des données à caractère personnel, adopté lors de la 267ème séance en novembre 1996[9].

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) :

- l'article 17 du Pacte international relatif aux droits civils et politiques (PIDCP) ;
- l'article 12 de la Déclaration universelle des droits de l'homme ;

[7] 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.
[8] *JO. L*281 du 23 novembre 1995, 31.
[9] *Protection of workers' personal data. An ILO code of practice*, Genève, OIT, 1997.

- les 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.

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 de la Constitution doit être interprété à la lumière de l'article 8 de la CEDH. Il ressort des travaux parlementaires que le but était que l'article 22 de la Constitution traduise 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 :

"§ 1. 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 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 travailleur et qui sont envoyés ou reçus par ses travailleurs est en principe 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[10].

33. Une majorité de la jurisprudence semble également partir du principe d'une interprétation stricte de l'article 314*bis* 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[11].

34. En outre, on peut argumenter que le contrôle de l'utilisation d'Internet, sous la forme d'un enregistrement des adresses de sites Internet (ce qu'on appelle "journaliser"), ne relève pas du champ d'application de cette disposition[12].

[10] 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.
[11] 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.
[12] 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.

36. La Commission considère la consultation par un employeur de données relatives à des courriers électroniques qui sont stockées sur le disque dur du travailleur ou sur un fichier géré par la personne chargée du contrôle comme étant effectuée après la transmission de la communication, et ne tombant donc pas dans cette hypothèse sous le coup de l'article 314*bis* du Code pénal[13].

b) Article 124 de la loi relative aux communications électroniques

37. L'article 124 de la loi *relative aux communications électroniques* du 13 juin 2005[14] (ci-après la "loi relative aux communications électroniques") dispose que "*S'il n'y est pas autorisé par toutes les personnes directement ou indirectement concernées, nul ne peut :*

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

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

39. 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).

[13] "*Le moment exact où s'achève la transmission d'une communication* (…)*, peut dépendre du type de service de communications électroniques fourni. Ainsi, dans le cas d'un appel par téléphonie vocale, la transmission cesse dès que l'un ou l'autre des usagers interrompt la connexion et, dans le cas d'un courrier électronique, la transmission prend fin dès que le destinataire récupère le message, généralement à partir du serveur de son fournisseur de service.*" Cf. la Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*.
[14] *M.B.* du 20 juin 2005.

40. 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 en principe punissable, sans qu'il ne soit question de la moindre intention.

41. 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 (article 124, 1° et 4° de la loi relative aux communications électroniques)[15].

42. 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 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 en principe punissable, même lorsqu'il prend fortuitement connaissance de ce courrier électronique.

43. La Commission estime qu'il y a uniquement interaction avec l'article 124 de la loi relative aux communications électroniques dans la mesure où l'on admet que l'employeur n'est jamais un co-destinataire de la communication électronique d'un travailleur (ce qui, selon certains, n'est pas le cas si le travailleur pose des actes juridiques numériques au nom et pour le compte de son employeur[16]) ou dans la mesure où l'on admet que la disposition prohibitive de l'article 124 de la loi relative aux communications électroniques s'applique jusqu'après la transmission du message (ce qui n'est pas le cas selon certains[17]).

---

[15] Cass., 1er octobre 2009, RG C.08.0064.N.

[16] Voir dans ce sens par exemple R. BLANPAIN, M. VAN GESTEL, Gebruik en controle van e-mail, intranet en internet in de onderneming, Praktijken Recht, Bruges, die Keure, 2003, n° 252 et 254.

[17] Voir dans ce sens par exemple le Conseil de la Concurrence dans l'Affaire MEDE-I/O-04/0063 et MEDE-I/O-06/0032 : les radiateurs en tôles d'acier, décision n° 2010-I/O-11 du 20 mai 2010. Dans cette affaire, ce Conseil vérifie si l'utilisation de copies de factures de téléphone mobile dans le cadre d'une enquête sur les pratiques restrictives de concurrence doit être qualifiée de prise de connaissance et d'utilisation au sens de l'article 124 de la loi relative aux communications électroniques. Le Conseil estime que la protection du secret des communications électroniques s'applique uniquement lors de la communication électronique :

c) Exceptions à l'interdiction légale

44. Le droit au respect de la vie privée n'est pas absolu[18] et la situation particulière du rapport hiérarchique entre l'employeur et le travailleur doit être prise en considération[19].

45. En outre, le travailleur ne peut pas invoquer sa vie privée uniquement pour échapper aux conséquences de son comportement frauduleux[20].

46. 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 illicite[21]. Le droit à la protection de la vie privée est un droit fonctionnel.

"83. Le Conseil estime que la disposition légale citée par Caradon vise en réalité la prise de connaissance d'informations (le contenu) envoyées par voie électronique et d'informations relatives à l'envoi par voie électronique pendant la transmission. En d'autres termes, la protection du secret des communications électroniques vise la protection pendant la communication électronique.
La nature des exceptions prévues à l'article 125 (voir ci-après) l'atteste : il est par exemple question d'écouter et d'utiliser les communications pour des interventions des services de secours, pour un contrôle de l'IPBT.
Les régimes particuliers en matière d'écoute prévus en droit pénal et cités par Caradon en attestent également. L'écoute ou l'enregistrement de conversations pendant la transmission est une mesure présentant un caractère intrusif pouvant entraîner une violation du secret de la communication.
84. Il n'est pas question ici de telles mesures car il s'agit de la prise de connaissance a posteriori de données relatives à une communication électronique au moyen de la prise de connaissance de traces écrites dans une facture.
85. Le Conseil estime que ce qui est également pertinent ici, c'est qu'il s'agit de factures de téléphone qui sont établies par l'opérateur à l'attention de l'abonné ou de l'utilisateur des services de cet opérateur. Il n'y a donc pas utilisation d'informations se trouvant encore sur le réseau mais uniquement utilisation des traces écrites de la relation contractuelle existant entre l'opérateur et l'utilisateur, à savoir via la facture. Cette facture contient la description des services fournis, à savoir les conversations effectuées avec mention du destinataire (les numéros), la durée et le moment. Il s'agit donc d'un élément dérivé de la communication elle-même sous la forme d'une facture a posteriori.
Le Conseil estime également pour cette raison que l'utilisation des factures ne tombe pas sous le coup du secret des communications électroniques au sens de l'article 124 de la loi relative aux communications électroniques.
86. En outre, il faut préciser que l'interprétation qui est donnée de cette disposition par Caradon, plus spécialement en ce qui concerne l'exigence du consentement, serait impossible dans la pratique et ne correspond pas à l'intention du législateur.
La mention de l'exigence du consentement étaie l'interprétation susmentionnée : il n'est judicieux de parler de consentement que lorsqu'il s'agit d'intervenir pendant la transmission. La thèse selon laquelle chaque personne concernée par une communication électronique devrait donner son consentement lorsqu'ultérieurement, des copies d'une facture sont utilisées, par exemple par une des personnes concernées elle-même , n'est pas envisageable dans la pratique."
[Traduction libre réalisée par le Secrétariat de la Commission, en l'absence d'une traduction officielle] Voir http://economie.fgov.be/fr/binaries/11_2010IO11_Staalplaatradiatoren_pub_tcm326-104598.pdf.

[18] Voir notamment Cass., 7 octobre 1981, *Arr. Cass.* 1981-82, 1983 ; Cass., 27 février 2001, *R.W.* 2001-2002, 1171.
[19] Cass., 27 février 2001, *A.J.T.* 2000-01, 949, note I. VERHELST.
[20] Voir par exemple C.T. Bruxelles, 22 juin 2000, *Computerrecht* 2001, 311.
[21] R. DE CORTE, "De achterkant van de privacy – Kan het beroep op privacy leiden tot straffeloos-heid?", *NJW.*, p. 808.

47. 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][22]. 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.

48. 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[23]. 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 aussi clairement moins grandes.

49. Sans préjudice de ce qui est précisé au point 43, les paragraphes suivants traitent les exceptions spécifiques aux dispositions de l'article 124 de la loi relative aux communications électroniques et de l'article 314*bis* du Code pénal.

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

50. 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 quant à la prise de connaissance.

51. 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.

[22] F. HENDRICKX, *Privacy en arbeidsrecht*, n° 1 de la Bijzondere reeks ICA, Bruges, die Keure, 1999, 200.
[23] Voir F. HEYNDRICKX, *Privacy en arbeidsrecht*, Bruges, die Keure, 1999, 51.

52. 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.

53. Bien qu'un employeur pourrait en théorie se baser sur le consentement du travailleur, il se pose en fait un problème quant à la qualité de ce consentement. Dans le cadre d'un contrat de travail, il n'y a pas d'équilibre entre les parties en présence (à tel point que le droit du travail 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[24]. Dans le domaine spécifique de la protection des données, seul un choix conscient et libre de la personne concernée peut légitimer le traitement de ses données à caractère personnel sur la base de l'article 5, a) de la LVP. Si le caractère volontaire du consentement n'est pas garanti, comme dans une relation de travail, cela annulera tout effet pertinent et protecteur de ce motif d'admissibilité pour traiter des données à caractère personnel. Si un employeur traite des données dans le cadre du contrôle de l'utilisation des moyens de communication patronaux, le consentement du travailleur n'est donc pas le bon fondement justificatif. Le traitement est alors la conséquence nécessaire et inévitable de la relation de travail. Dans ce cas, il est même fallacieux de légitimer le traitement par le consentement du travailleur[25]. Étant donné que le traitement envisagé est inhérent au contrôle de l'employeur, le travailleur ne peut évidemment pas se soustraire au traitement par le seul fait de ne pas donner son consentement ou de retirer ultérieurement un consentement donné. Un consentement éventuel du travailleur ou l'absence de celui-ci n'ajoute ou ne retire rien au principe du droit de l'employeur de contrôler l'usage fait par les travailleurs des moyens de communication en ligne mis à leur disposition, de prendre connaissance de leurs données de communication en ligne et de traiter ces données à caractère personnel, lorsque ces traitements sont nécessaires en vue de l'exécution d'obligations et de droits spécifiques de l'employeur en ce qui concerne le droit du travail. Au lieu de se concentrer sur le consentement soi-disant indispensable du travailleur en vertu de la législation en matière de télécommunications (et qui créera tout au plus un système artificiel de justification pour le traitement), les intérêts de la vie privée d'un travailleur individuel qui est sous autorité peuvent, selon la Commission, être mieux protégés d'une autre manière :

[24] "*Par "consentement de la personne concernée", on entend toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.*" (article 1, § 8 de la LVP). Dans la Directive 2002/58/CE (transposée dans la loi relative aux communications électroniques), *le "consentement d'un utilisateur ou d'un abonné", que ce dernier soit une personne physique ou une personne morale, devrait avoir le même sens que le "consentement de la personne concernée" tel que défini et précisé davantage par la directive 95/46/CE* (voir le considérant n° 17 de la Directive 2002/58/CE).

[25] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48fr_sum.pdf. Il s'agit d'une note de synthèse d'un 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 regroupe les autorités de contrôle et de protection des données de tous les États membres de l'Union européenne.

- tout d'abord en utilisant les instruments de négociation et de concertation développés entre employeurs et travailleurs dans le cadre du droit social, qui ont justement pour but d'atténuer les conséquences de cette relation inégale ;

- ensuite en rendant la politique de contrôle menée par le patronat 'prévisible' pour les membres du personnel eux-mêmes au sens exigé par l'article 8 de la CEDH, à savoir en spécifiant cette politique dans une procédure qui tienne compte de l'ensemble des normes applicables en cette matière (LVP, loi relative aux règlements de travail, le cas échéant, CCT n° 81, ...).

54. 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[26].

2° Exceptions techniques

55. 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.

56. Certains auteurs ont interprété l'exception dont question comme permettant des interventions nécessitées sur le réseau de l'entreprise[27].

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

- 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) ;

[26] Trib. trav. Bruxelles, 4 décembre 2007, *J.T.T.* 2008, n° 1005, 179.
[27] 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.

- 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).

58. 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 dans l'entreprise. Toutefois, bien que la portée de ces exceptions légales spécifiques soit limitée pour les employeurs réguliers, cela n'empêche pas que cet article illustre en fait l'idée que l'employeur doit finalement pouvoir traiter de manière plus souple des données de communication de travailleurs ayant un caractère professionnel que des données de communication de travailleurs ayant un caractère privé. Ou, à l'inverse, que lors du traitement de données de communication de travailleurs ayant un caractère personnel, davantage de garanties devront être offertes.

59. En outre, il ne faut pas oublier que ces exceptions légales spécifiques concernent la prise de connaissance du contenu pendant la transmission de la communication – une mesure présentant un caractère particulièrement intrusif dans le cadre de laquelle le secret de la communication peut être violé – alors que les employeurs réguliers souhaitent 'uniquement' s'assurer que la communication personnelle accomplie ne compromet pas l'exécution du contrat de travail de la personne concernée (par la prise de connaissance des données de trafic) ou souhaitent seulement accéder au contenu de communications électroniques professionnelles qu'un travailleur a déjà reçues pendant son absence pour pouvoir assurer la continuité du service pendant cette absence. Cette nuance est assez importante.

3° Autorisation légale

60. L'article 125, § 1, 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[28].

61. 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 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

[28] Dans ce cas, les articles 259*bis* et 314*bis* du Code pénal ne sont pas non plus d'application.

le droit de contrôle de l'employeur. Bien entendu, cela s'applique également aux agents qui travaillent sous autorité, en vertu d'un statut.

62. 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.

63. 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 ; (…)".

64. La jurisprudence semble d'avis que ces dispositions peuvent constituer l'exception légale requise[29].

65. La Commission estime également que c'est le cas et précise d'emblée que cela vaut aussi pour les dispositions légales similaires qui, tout comme la loi relative aux contrats de travail, traduisent l'autorité des employeurs du secteur public, comme par exemple les articles 120 et 124 de la loi du 7 décembre 1998 *organisant un service de police intégré, structuré à deux niveaux* et l'article 7, § 1 de l'arrêté royal du 2 octobre 1937 *portant le statut des agents de l'État.*

66. Chaque employeur a une mission légale générale en matière de contrôle et de surveillance de son personnel, et donc aussi de l'utilisation que les travailleurs font des moyens de communication (en ligne) mis à leur disposition. La politique de contrôle patronale menée doit évidemment être rendue plus "prévisible" pour les membres du personnel, à savoir en spécifiant cette politique dans un règlement. L'employeur devra également toujours exercer son droit d'autorité dans les limites des exceptions et des garanties décrites entre autres dans la LVP. Cela ne veut toutefois pas encore dire

[29] 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.

que la définition de l'autorité formulée en général, par exemple dans la loi relative aux contrats de travail, serait insuffisante en soi.

67. Comme déjà précisé, pour certaines méthodes de surveillance patronale, telles que l'écoute ou l'enregistrement systématique de communications pendant la transmission (par exemple conversations téléphoniques complètes), un encadrement légal spécifique est déjà disponible pour certains milieux professionnels. Par exemple, la base légale dans le secteur de la bourse/des investissements/des call centers, pour écouter systématiquement en temps réel les conversations téléphoniques de membres du personnel est reprise spécifiquement dans la loi relatives aux communications électroniques (article 128). Étant donné qu'il s'agit ici clairement d'une "ingérence" plus poussée, une exception légale particulière a donc été décrite sur ce point pour ces environnements de travail dans la loi relative aux communications électroniques elle-même. La légitimité générale de tels actes de contrôle dans les milieux en question a donc été reconnue dans la loi relative aux communications électroniques elle-même et ne peut donc pas être qualifiée ainsi de disproportionnée sur la base par exemple de l'article 4 de la LVP. De tels actes, s'ils sont de nature systématique, ne sont par contre pas justifiables pour des employeurs réguliers uniquement sur la base de leur mission générale en matière de contrôle et de surveillance de leurs travailleurs (et même s'ils l'étaient, ils pourraient encore toujours être considérés comme disproportionnés). Toutefois, cela signifie *a contrario* que le législateur a donc également dû être d'avis que pour des actes moins intrusifs au sens de l'article 124 de la loi relative aux communications électroniques, tels que l'établissement et la prise de connaissance de télécommunications effectuées, la disposition de contrôle légale générale dont dispose chaque employeur est en principe adéquate, comme par exemple le contrôle et l'accès aux courriers électroniques dans la boîte de messagerie d'un utilisateur.

68. Il va de soi que ce droit de l'employeur d'exercer une autorité, formulé de manière générale, peut uniquement servir de fondement légal pour poser certains actes de contrôle, pour autant que ceux-ci se déroulent conformément à la gestion habituelle normale de l'entreprise (en tant qu'employeur raisonnable et prudent[30]) et conformément à d'autres dispositions pertinentes applicables au niveau légal (telles que la LVP et la loi du 8 avril 1965 *instituant les règlements de travail*[31]) et au niveau réglementaire (telles que l'arrêté royal du 27 août 1993 *relatif au travail sur des équipements à écran de visualisation*[32]) et à des dispositions de certaines conventions collectives de travail (telles que

[30] Comme requis légalement notamment par l'article 1134, alinéa 3 du Code civil (bonne foi), l'article 1382 du Code civil (obligation de minutie). Le respect des principes généraux de bonne gouvernance qui s'appliquent à un employeur de la fonction publique empêchent également que celui-ci n'agisse pas comme un employeur prudent.

[31] La loi du 8 avril 1965 prévoit et légitime également la surveillance au travail. Mais elle oblige surtout que le contrôle et la surveillance que l'employeur pourrait exercer, ainsi que les conséquences éventuelles de ceux-ci pour le travailleur, soient réglementés au sein de l'entreprise/l'administration.

[32] L'arrêté royal de 1993 prescrit dans son annexe qu'on ne peut faire usage d'un mécanisme de contrôle quantitatif ou qualitatif à l'insu des travailleurs. *A contrario*, cet arrêté royal autorise donc les employeurs à utiliser un mécanisme de contrôle quantitatif ou qualitatif si les travailleurs en sont informés. Cela ne sera possible que grâce à l'enregistrement et/ou la prise de connaissance de

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*, la CCT n° 9 du 9 mars 1972 *coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprises, conclus au sein du Conseil national du travail* et la CCT n° 39 du 13 décembre 1983 *concernant l'information et la coopération sur les conséquences sociales de l'introduction des nouvelles Technologies*).

69. 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. (…)".

70. 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[33]. Le fait que le préposé a agi sur le lieu de travail et pendant les heures normales de service est considéré comme déterminant[34]. Cette large interprétation a pour conséquence que le commettant est également responsable en cas d'abus de la fonction[35] et qu'il est également tenu pour responsable du dommage causé par un délit du préposé[36].

71. 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

certaines données, donc via un traitement de données à caractère personnel. Cet arrêté royal ne parle nullement d'un consentement des travailleurs par exemple. Ce texte réglementaire illustre que des actes de contrôle du comportement numérique des travailleurs effectués par l'employeur dans le cadre de sa mission générale de surveillance sont en principe légitimes.

[33] 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.

[34] Voir notamment H. VANDENBERGHE, M. VAN QUICKENBORNE et P. HAMELINK, "Overzicht van rechtspraak (1964-1978), *TPR* 1980, 1336.

[35] 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.

[36] Voir Cass. 9 février 1982, *Arr. Cass.* 1981-1982, 741.

72. 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 au Conseil National du Travail.

73. Vu la hiérarchie des normes juridiques, 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*".

74. 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*".

75. 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*".

76. Par données de communication électroniques en réseau, on vise aussi, selon la Cour du travail de Bruxelles, les courriers électroniques enregistrés[37].

77. 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.

78. 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.

[37] C.T. Bruxelles, 13 septembre 2005, *Computerr. (Ned.)* 2006, n° 2, 100.

79. 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)

80. 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[38].

2° la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ;

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

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

[38] C.T. Anvers (Sect. Hasselt), 15 novembre 2005, *Soc. Kron.* 2006, 153.

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*[39]. 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)

81. 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.

82. 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 électroniques en réseau de l'entreprise ;
- les sanctions prévues dans le règlement de travail en cas de non-respect des règles.

83. 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 donc pas obligatoirement être reprises dans le règlement de travail. C'est uniquement le cas si

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

le contrôle est effectué en vue de mesurer le travail ou s'il concerne les compétences du personnel de surveillance (article 6, § 1, 5° de la loi relative aux règlements de travail) 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

84. 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

85. 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)

86. 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).

87. 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.

88. 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 ;
- messagerie 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.

89. 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

90. 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"*.

91. 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.

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

g) Procédure directe

93. Une individualisation directe est autorisée lorsque l'employeur poursuit l'une ou plusieurs des finalités 1°-3° mentionnées au point 80.

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

95. Des irrégularités 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

96. Si l'employeur poursuit la finalité visée au point 4° du point 80, une procédure spécifique doit être suivie avant de pouvoir procéder à l'individualisation.

97. 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 claire et compréhensible, l'existence de l'irrégularité et de les avertir d'une individualisation des données de communication électroniques en réseau lorsqu'une nouvelle irrégularité 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 en vigueur dans l'entreprise de manière à éviter la survenance d'une nouvelle anomalie de même nature.

98. Lorsque par la suite, un travailleur individuel est tenu pour responsable d'une (nouvelle) irrégularité, 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.

99. En ce qui concerne l'interaction entre cette CCT et un certain nombre de normes juridiques supérieures, on peut rappeler que le fondement légal de l'intrusion patronale dans la vie privée, les données à caractère personnel et les (données de) communications électroniques de travailleurs est fourni par les dispositions légales contraignantes relatives à l'autorité de l'employeur (voir ci-dessus) tel qu'autorisé sur la base de l'article 125, § 1, 1° de la loi relative aux communications électroniques ("lorsque la loi le permet ou l'impose"). L'employeur dispose du droit/pouvoir disciplinaire dans son entreprise/administration et le contrôle des actes numériques des travailleurs se fait en première instance dans ce but qui tombe clairement sous le coup du droit du travail. Dans ce cadre, le contrôle patronal des données de messagerie électronique et d'Internet sur le lieu de travail doit être adéquat et nécessaire, se faire à des fins légitimes et être transparent. Ces obligations fondamentales découlent notamment de la LVP – le fondement de tout traitement de données à caractère personnel – et ces

devoirs sont spécifiés par la CCT n° 81 [40] en ce qui concerne précisément le contrôle des communications en réseau sur le lieu de travail. Il s'ensuit donc que les dispositions essentielles de cette CCT, bien qu'une CCT ne soit formellement pas applicable au secteur public, ne peuvent pas être tout simplement ignorées par les employeurs de ce secteur. La principale spécification dans la CCT est l'imposition d'un contrôle hiérarchisé des données de communication électroniques personnelles en application de l'article 4, § 1, 3° de la LVP : il faut notamment qu'un usage privé non souhaité, illégitime ou punissable soit constaté à l'occasion d'un contrôle global, avant de pouvoir imputer ces données de communication personnelles à un travailleur spécifique (que ce soit ou non via une procédure directe) et en principe, l'individualisation se limite aux données de télécommunications elles-mêmes et pas à leur contenu. Il n'est dès lors pas concevable que dans le secteur public, un contrôle des données de communication électroniques personnelles qui peuvent être imputées à un travailleur déterminé puisse *a priori* avoir lieu, et encore moins que le contenu de telles données personnelles soit systématiquement individualisé. Ce non respect de ce principe de proportionnalité dans la fonction publique serait en effet non seulement contraire à la LVP mais également à l'article 1134, alinéa 3 du Code civil (bonne foi), à l'article 1382 du Code civil (obligation de minutie) et aux principes généraux de bonne gouvernance qui empêchent également qu'un employeur public agisse comme un employeur négligent.

100. La distinction que la CCT fait entre les données de communication relatives à un travailleur (et son correspondant) qui surviennent en exécution de son contrat de travail et les données personnelles relatives à un travailleur (et son correspondant) qui surviennent (messages reçus et envoyés) dans l'accomplissement de la vie privée de la personne concernée sur le lieu de travail ("Niemitz") repose sur le principe de pertinence de la LVP[41]. La LVP doit évidemment s'appliquer aux deux catégories de données[42] car ce sont toutes deux des données à caractère personnel. Le degré de

[40] Réponse du vice-premier ministre et ministre de l'Emploi à la demande d'explication de monsieur Vincent Van Quickenborne (n° 2-788) sur la "validité juridique de la CCT n° 81 qui tend à protéger la vie privée des travailleurs par rapport au contrôle des données électroniques de communication en ligne", Sénat belge, Actes, 23 mai 2002 : " *(…) On ne fixe pas des règles nouvelles ou supplémentaires pour garantir la protection de la vie privée. Les règles existantes sont simplement précisées et concrètement appliquées pour le cas où l'employeur voudrait contrôler et traiter l'utilisation des données sur le lieu de travail. En réponse à votre première question, je peux vous dire que la CCT n° 81 est compatible avec l'article 22 de la Constitution, étant donné que la protection du droit au respect de la vie privée et familiale n'est pas le moins du monde réglée, mais simplement précisée. Pour cela, une loi au sens formel du terme n'est pas nécessaire. Vous m'avez demandé si la convention sera rendue obligatoire. Elle sera traitée comme toutes les autres conventions collectives de travail. Le contenu fera tout d'abord l'objet d'un contrôle afin de déterminer s'il est conforme aux normes nationales, européennes et internationales valables en la matière. Si, au terme d'un tel contrôle, aucune objection n'est émise et aucun problème n'est décelé, la convention sera rendue obligatoire. Enfin, je ne peux actuellement pas vous donner une réponse définitive à votre troisième question. On doit auparavant déterminer s'il est utile et opportun de créer, à côté de la législation déjà existante, un nouveau texte de loi distinct, relatif aux droits et devoirs des employeurs et des travailleurs en ce qui concerne les e-mails et l'utilisation d'Internet au travail en général. Je souhaite encore une fois insister sur le fait que la CCT n° 81 consiste seulement en une précision de la réglementation déjà existante, qui est applicable tant aux entreprises privées qu'aux institutions publiques.*"

[41] Tout cela implique qu'un collaborateur a déjà entrepris une démarche active en spécifiant que le courrier électronique concerné est de nature professionnelle (ou justement pas).

[42] L'article 11, troisième alinéa de la CCT stipule que les règles d'individualisation de la CCT ne s'appliquent pas à cette catégorie de données mais pas que la LVP ne serait pas d'application. C'est probablement le rapport de la CCT qui est formulé de manière quelque peu ambigüe sur ce point : "*Dans cette mesure et lorsque l'objet et le contenu des données de communication*

protection en vertu de la LVP est en effet le même pour toutes les données (les données personnelles aussi bien que les données professionnelles), compte tenu que cette protection équivalente autorise que certaines données soient traitées licitement et légitimement par l'employeur (au moyen de la prise de connaissance patronale), et que d'autres ne puissent éventuellement pas l'être. À cet égard, des données qui surviennent en exécution du contrat de travail sont, en soi, pertinentes pour l'employeur, également en ce qui concerne leur contenu. Seul un accès au contenu d'un message électronique professionnel peut assurer que l'employeur réalise sa finalité (par exemple la poursuite de la correspondance professionnelle en l'absence d'un travailleur). Des données de communication personnelles sont par contre excessives en des circonstances normales et ne peuvent donc pas être connues de l'employeur. Elles ne sont pertinentes pour l'employeur, en premier lieu, qu'en ce qui concerne leur existence, dans la mesure où elles compromettent la bonne exécution du contrat de travail ou le statut de la personne concernée (à savoir en cas de communication personnelle punissable, illégitime ou non autorisée). Sinon, l'employeur reste non habilité à procéder au traitement et des données de communication personnelles individualisées ne peuvent pas être portées à sa connaissance.

101. Bien que l'étendue de l'accès à des données de communication électroniques personnelles en réseau soit donc plus limité par rapport à l'accès à des données de communication électroniques professionnelles en réseau (on ne peut en principe pas prendre connaissance du contenu), un tel accès doit donc être encadré de plus de garanties pour la personne concernée, en vertu du principe de proportionnalité (application d'un contrôle hiérarchisé et individualisation uniquement lorsqu'à l'occasion d'un contrôle général, des abus et des irrégularités ont été constatés), précisément parce qu'un tel accès implique le contrôle de mouvements de communications privées qui s'inscrivent par excellence dans le contexte de la protection de la vie privée du travailleur. Le régime d'accès plus strict à ce type de (données de) communications électroniques va ainsi de pair avec l'augmentation des risques en matière de vie privée pour la personne concernée.

102. Cela implique également qu'un employeur ne peut pas directement prendre connaissance du contenu d'une communication électronique. Compte tenu du fait qu'une boîte de réception peut toujours contenir des informations non professionnelles, il est préférable de travailler avec une personne de confiance intermédiaire, même lorsque les boîtes de réception se trouvent sur un serveur de l'employeur : un 'firewall' humain entre l'employeur et le travailleur qui bénéficie de la confiance légitime des deux parties, avec une indépendance suffisante vis-à-vis de l'employeur et une attention particulière au 'dépassement des compétences' dans le chef des deux parties. L'intervention de cette personne peut par exemple empêcher que l'employeur puisse déjà contrôler *a priori* au niveau de l'utilisateur en ce qui concerne l'abus non désiré, illégitime ou punissable des moyens en ligne en

électroniques en réseau ont un caractère professionnel non contesté par le travailleur, l'employeur pourra les consulter ***sans autre procédure***."

contradiction avec les principes de la CCT n° 81. Cette personne de confiance, par exemple un préposé à la protection des données, ne peut en effet transmettre au management aucune donnée de communication individualisée sur des travailleurs sans raison légitime en vertu de l'obligation de discrétion. L'intervention de cette personne empêche par exemple également qu'un employeur qui, dans le cadre de sa quête légitime de certains messages électroniques professionnels, accède à la boîte de messagerie d'un membre du personnel (absent) ne puisse lire en même temps le contenu des messages personnels de celui-ci. Enfin, cette personne pourrait également vérifier si le label 'privé' qui a été indiqué par un travailleur dans la ligne 'objet' d'un courrier électronique déterminé l'a été de bonne foi (dans le cadre de l'exercice légitime de son droit au respect de la vie privée) ou s'il a servi de prétexte pour nuire aux intérêts de l'employeur de manière illégitime ou punissable. Dans le premier cas, le courrier électronique contrôlé reste confidentiel vis-à-vis du management et dans l'autre cas, il est bel et bien transmis au management pour suite utile. En bref, cette personne de confiance pourrait uniquement sélectionner les informations qui sont *a priori* réellement nécessaires et les transmettre à l'employeur

4. Article 550*bis* du Code pénal

103. L'article 550*bis*, § 1, du Code pénal punit d'un emprisonnement de 3 mois à 1 an et/ou d'une amende de 26 euros à 25.000 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.

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

105. 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/ou une amende de vingt-six euros à vingt-cinq mille euros.

106. 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/ou d'une amende de vingt-six euros à cinquante mille euros)".

107. 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.

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

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

109. La Commission entend rappeler très fermement l'application de la LVP dont les dispositions contraignantes 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.

110. 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.

111. 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*".

112. 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 physique identifiée ou identifiable.

113. 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).

114. 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.

115. À l'occasion de tels traitements, 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.

116. La LVP impose aux 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.

117. 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[43].

118. 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 communication 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.

119. Ces **finalités** doivent en outre être **légitimes**. L'article 5 de la LVP énumère 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.

120. À cet égard, la Commission estime qu'un traitement de données réalisé dans le cadre 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).

121. Comme déjà précisé, la Commission estime que le consentement du ou des travailleurs concernés ne peut toutefois 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.

122. L'arrêté royal du 13 février 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-*

[43] Article 4, § 1, 2° de la LVP.

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"[44].

123. 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.*"[45].

124. 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 (par exemple surveiller le respect des instructions par le travailleur) et éventuellement, en outre, par la réalisation de l'intérêt légitime poursuivi par l'employeur (par exemple 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.

125. 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, § 1, 5° de la LVP).

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

127. 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 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

[44] 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*.
[45] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48fr_sum.pdf. Il s'agit d'une note de synthèse d'un 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 regroupe les autorités de contrôle et de protection des données à caractère personnel de tous les États membres de l'Union européenne.

disposition contienne des mesures appropriées, garantissant la sauvegarde des intérêts légitimes de la personne concernée. Ainsi, il devra au moins être permis à cette dernière de faire valoir utilement son point de vue.

128. 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 du traitement et qui se traduit par l'obligation de fournir certaines informations aux travailleurs concernés notamment sur la finalité du traitement (article 9 de la LVP). Si le contrôle est effectué à des fins légitimes au su des utilisateurs concernés, on ne peut pas parler de l'utilisation d'un logiciel espion dans le chef de l'employeur. Voir à cet égard également l'arrêté royal du 27 août 1993 *relatif au travail sur des équipements à écran de visualisation,* qui prescrit qu'au su des travailleurs, un dispositif de contrôle quantitatif et qualitatif peut être utilisé. Enfin, il y a l'obligation de déclarer préalablement le traitement à la Commission[46]. S'il existe des exceptions à ces deux obligations, la Commission estime qu'elles ne sont *a priori* pas applicables en l'espèce[47].

129. 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**[48] et que la **sécurité du traitement est assurée**[49], notamment en cas de sous-traitance de certaines opérations de traitement, afin notamment d'empêcher une réutilisation 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°).

130. Il devra également se conformer à toutes les autres obligations imposées par la LVP.

II.3. CONCLUSION

[46] Voir à cet égard les articles 9 et 17 de la LVP.
[47] Voir 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.
[48] Il s'agit des droits d'accès, de rectification et d'opposition tels que décrits aux articles 10, 11 et 12 de la LVP.
[49] Voir à cet égard les obligations décrites à l'article 16 de la LVP.

131. 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, et donc également leurs actes numériques. 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.

132. 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.

133. 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).

134. 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.

135. La Commission estime que ces dispositions, ou des dispositions similaires dans la fonction publique, ainsi que les directives établies dans la LVP et 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, lues conjointement, constituent une autorisation légale au sens de l'article 125, § 1, 1° de la loi relative aux communications électroniques, ce qui exclut toute violation de l'article 124 de la loi relative aux communications électroniques, pour autant que l'employeur respecte les trois principes de base de ces législations, dont le respect est jugé essentiel pour la protection de la vie privée des travailleurs lors d'un traitement de leurs données à caractère personnel : le principe de finalité, le principe de proportionnalité et le principe de transparence.

136. 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 la transmission de la communication, comme requis pour être punissable en application de l'article 314*bis* du Code pénal.

137. 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.

138. La Commission énumère ci-après les principes de base susmentionnés auxquels l'employeur doit se conformer lors de l'exercice de son droit de contrôle.

Principe 1 : principe de finalité

139. 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.

140. 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 quoi sert le contrôle et selon quelles modalités les éventuelles données traitées pourront être/seront utilisées 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.

141. 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 prévisions 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

142. 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

143. 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 ILLICITEMENT)

144. Bien que l'employeur ait intérêt à mettre en œuvre et à respecter correctement les conditions, procédures et garanties légales précitées, étant donné que les preuves recueillies lors des contrôles qu'il aura effectués seront alors normalement considérées comme valables en droit, la Cour de cassation a estimé dans l'arrêt dit "Antigone" du 14 octobre 2003 qu'une preuve obtenue illicitement ne doit donner lieu à l'exclusion que si le respect de certaines exigences de forme est prescrit à peine de nullité, si l'illicéité commise a entaché la fiabilité de la preuve ou si l'usage de la preuve est contraire au droit à un procès équitable[50]. 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"*[51].

145. La Cour européenne des droits de l'homme a également déjà approuvé cette jurisprudence[52].

146. 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

[50] Cass. 14 octobre 2003, RG P.03.0762.N, avec conclusions de M. l'avocat général DE SWAEF.
[51] Cass. 23 mars 2004, RG P.04.0012.N.
[52] 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.

d'apprécier les conséquences de cette méconnaissance sur la recevabilité des moyens de preuve obtenus de façon irrégulière[53].

147. Dans son arrêt du 10 mars 2008[54], 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 illicitement à la lumière des articles 6 de la CEDH et 14 du Pacte international relatif aux droits civils et politiques 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'illicéité 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'illicéité 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'illicéité commise ;
- le fait que la preuve recueillie illicitement concerne uniquement un élément matériel de l'existence de l'infraction ;
- le fait que l'illicéité qui a précédé ou contribué à la constatation de l'infraction est hors de proportion avec la gravité de celle-ci.

148. 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.

149. Ces principes ont également déjà été bien accueillis par les juridictions du travail. Ainsi, dans son jugement du 1er septembre 2008[55], 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 pas été annoncé. Le tribunal du travail a constaté qu'en dépit de cette illégitimité, la

[53] Cass. 2 mars 2005, *Arr. Cass.* 2005, n° 3, 506, concl. VANDERMEERSCH; *Rev.dr.pén.* 2005, n° 6, 668.
[54] *Pas.* 2008, n° 3, 652 ; *RCJB* 2009, n° 3, 325.
[55] TGR-TWVR 2009, n° 4, 275.

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[56]. Depuis lors, plusieurs décisions ont fait application de la jurisprudence dans les litiges sociaux[57].

150. 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").

151. 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.

152. 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.).

153. Enfin, la Commission rappelle que les violations de la LVP peuvent également être sanctionnées d'une autre manière que par l'exclusion (avec ou sans examen des intérêts par le juge du fond) de la preuve. La LVP contient une série de dispositions pénales (en particulier l'art. 39 de la LVP). L'employeur qui traite des données en contradiction avec la LVP s'expose dès lors à des poursuites pénales. Il existe déjà une jurisprudence où la preuve obtenue illicitement n'a pas été rejetée des débats, étant donné la gravité des faits établis par la preuve, mais où l'employeur était en même temps condamné du chef de violation des règles sur la vie privée.

IV. RECOMMANDATIONS

154. La Commission formulera ci-après, sous la forme de recommandations, une série de bonnes pratiques qui constituent autant d'exemples ou de moyens de tenir compte de la LVP dans le cadre d'un accès à des moyens de communication électroniques et qu'elle considère à même de prévenir les conflits entre les intérêts des employeurs et la protection des droits des travailleurs.

---

[56] *Or.* 2008, n° 9, 261.
[57] Voir 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.

155. De manière générale, et sous réserve de leur mise en œuvre dans la pratique, ces recommandations doivent permettre de garantir l'adéquate protection des droits et libertés fondamentaux de toutes les personnes dont les données à caractère personnel sont traitées dans le cadre d'un accès à des moyens de communication électroniques.

156. La Commission tient toutefois à préciser que ces recommandations n'ont aucun caractère impératif ou obligatoire. Les recommandations énumérées constituent uniquement un fil conducteur. On peut en effet envisager d'autres exemples/suggestions peut-être plus adaptés à la spécificité de certaines entreprises ou fonctions, qui peuvent également représenter le contenu ou la traduction concrète de certaines règles ou obligations légales qui découlent de la LVP.

157. La Commission n'entend pas, à cet égard, se substituer aux employeurs, responsables des traitements de données à caractère personnel effectués lors du contrôle ou de la surveillance de leurs travailleurs, ni aux partenaires sociaux, qui ont le pouvoir et la compétence pour négocier des règles en matière d'organisation de ce contrôle et de cette surveillance et de conclure des accords, dans le respect des règles légales contraignantes.

158. C'est d'autant plus le cas, vu la diversité entre et au sein d'administrations et d'entreprises. Une politique interne devra finalement concrétiser de quelle manière (procédurale) l'ensemble des garanties consignées entre autres dans la LVP seront offertes et respectées dans la pratique par l'employeur, afin de préserver en cas de contrôle/accès, le droit à la protection de la vie privée des travailleurs prévu par l'article 2 de la LVP[58].

159. Nous formulons ci-après plusieurs règles de conduite **juridiques** autour de quatre thèmes qui constituent des exemples ou des outils permettant de tenir compte de la LVP lors d'un accès patronal à des communications électroniques ou d'un contrôle de ces dernières.

160. À titre de recommandation générale de base, il convient d'élaborer au maximum des règles préventives (sur le plan juridique, en lien avec le management et sur le plan technique) ainsi que des procédures préventives (par exemple pour le classement de courriers électroniques, de documents, de fichiers) afin d'éviter que survienne le besoin dans le chef de l'employeur de contrôler et d'accéder à des informations personnelles des travailleurs.

161. En la matière, si l'employeur a un rôle à jouer, c'est également le cas des personnes concernées elles-mêmes. Les membres du personnel sont tenus à un devoir de rigueur en ce qui concerne leurs propres données à caractère personnel disponibles sur le lieu de travail (par exemple,

[58] "*Lors du traitement de données à caractère personnel la concernant, toute personne physique a droit à la protection de ses libertés et droits fondamentaux, notamment à la protection de sa vie privée.*"

des données relatives à des évaluations, des fiches de salaire, …) et doivent dès lors les protéger suffisamment à l'égard de tiers, et ce même au sein de l'entreprise ou de l'administration publique.

162. Cela vaut par exemple aussi pour des courriers électroniques privés reçus ou envoyés sur le lieu de travail. Les travailleurs utilisent en effet aussi le système de messagerie électronique de l'employeur à des fins privées, dans une plus ou moins grande mesure, surtout si cela a été explicitement autorisé par l'employeur.

163. Les travailleurs ont certes le droit d'effectuer des communications privées sur le lieu de travail, dans une mesure limitée, mais pour protéger leur vie privée, mieux vaut séparer autant que possible les courriers électroniques professionnels des courriers électroniques privés.

164. Les courriers électroniques privés reçus ou envoyés pendant les heures de travail par le travailleur ne sont en effet *a priori* pas destinés à être lus ou reçus par l'employeur, et certainement pas en ce qui concerne leur contenu[59].

165. Les courriers électroniques fonctionnels doivent par contre *a priori* pouvoir être traités dans le contexte normal de communication professionnelle au sein d'une entreprise/administration publique – et il en va de même en ce qui concerne leur contenu –, étant donné qu'ils concernent évidemment l'exécution de la tâche de travail au sens strict.

166. En cas de double utilisation du système de messagerie électronique, il est toutefois difficile de concilier les droits et intérêts des deux parties.

167. Dans ce cas, bien que l'intention de l'employeur se limite à la prise de connaissance du contenu des courriers électroniques à caractère professionnel en vue de la gestion et de l'organisation de ses activités (et non en vue de "contrôler" un quelconque abus du système de messagerie électronique), cet employeur portera quoi qu'il en soit atteinte à la vie privée de l'utilisateur final.

168. En effet, il sera inévitablement confronté à des courriers électroniques non professionnels, alors que la prise de connaissance de l'existence de tels courriers électroniques (sans parler de leur contenu) ne serait en fait possible qu'à la suite de l'approche graduelle de la CCT n° 81 (d'abord un contrôle anonyme et ensuite, un contrôle individualisé) et moyennant le respect des règles d'individualisation prévues par cette CCT.

[59] Toutefois, du fait qu'ils sont générés pendant les heures de service, l'employeur doit pouvoir suivre l'existence de certaines communications privées de ses subalternes lorsqu'elles compromettent la bonne exécution de la tâche de travail (abus des heures de travail).

169. Dans un tel contexte, une solution est évidente : elle consiste à éviter la double utilisation du système de messagerie électronique de l'employeur. Le problème de l'accès direct aux courriers électroniques privés des travailleurs ne se pose ainsi normalement plus.

170. Cette méthode peut être appliquée en demandant aux travailleurs d'utiliser une adresse de messagerie personnelle (de type Hotmail) pour leurs courriers électroniques privés, et non l'adresse de messagerie électronique mise à leur disposition pour pouvoir exécuter les activités professionnelles.

171. Si l'employeur a précisé dans sa politique ICT que le double usage de son système de messagerie électronique (professionnel et privé) est interdit, il peut en principe considérer que les courriers électroniques ont un caractère professionnel, surtout en ce qui concerne les messages envoyés[60].

172. Un éventuel accès direct à de tels courriers électroniques d'un travailleur peut dès lors se justifier, moyennant le respect des grands principes de base de la LVP, à savoir un accès limité à des finalités déterminées, explicites et légitimes ; cet accès doit en outre être adéquat, pertinent et non excessif au regard des finalités et à condition d'avoir fourni des informations adéquates quant à cet accès.

173. Si l'employeur tombe néanmoins sur un courrier électronique privé lors d'un tel accès direct, il en prend connaissance de manière licite, étant donné qu'aucune mesure spécifique ne devait être prise pour protéger des informations privées (qui ne pouvaient en principe pas s'y trouver). Cela ne signifie pas pour autant qu'un courrier électronique privé dont l'employeur prend ainsi connaissance puisse ensuite être utilisé pour un but quelconque (par exemple, une utilisation dans une intention frauduleuse ou en vue de nuire au travailleur en question ou à un tiers). Une utilisation ultérieure de ce courrier électronique devra par contre respecter les exigences de la LVP.

174. Lorsque les employeurs ne peuvent ou ne veulent pas abandonner la double utilisation de leur système de messagerie électronique, ils devront inévitablement accepter qu'un membre du personnel puisse faire valoir des attentes supérieures en matière de vie privée à l'égard de sa boîte de réception électronique. En cas d'usage mixte du système de messagerie électronique du patron par le travailleur, des mesures spécifiques devront donc être prises par l'employeur qui tendront à épargner et protéger autant que possible les messages personnels de l'intéressé dans le cadre de la recherche de messages professionnels (sur lesquels l'employeur a manifestement un droit).

[60] En ce qui concerne les courriers électroniques entrants, l'employeur devra être plus prudent qu'à l'égard des courriers électroniques sortants, étant donné que le travailleur n'en est pas l'auteur et n'attendait évidemment même pas certains d'entre eux.

175. Une telle boîte de réception mixte ne peut dès lors pas être consultable directement et intégralement par l'employeur. Il faudra par contre convenir d'une procédure complémentaire pour faire la distinction entre les deux types de messages, par exemple en demandant au travailleur de classer les courriers électroniques reçus et envoyés. La prise de connaissance patronale de l'existence de courriers électroniques classés comme étant privés (sans parler de leur contenu) ne serait alors en fait possible qu'à la suite de l'approche graduelle de la CCT n° 81 et moyennant le respect des règles d'individualisation prévues par cette CCT.

176. Les recommandations juridiques suivantes s'appliquent dès lors surtout, mais pas exclusivement, aux employeurs qui permettent ou tolèrent la double utilisation de leur système de messagerie électronique.

Assurez-vous du respect du principe de légitimité, de la prévisibilité des traitements et de l'ingérence dans le droit au respect de la vie privée des travailleurs

- ne traitez des données à caractère personnel que dans les cas autorisés par la LVP ;

- prévoyez une participation et une consultation de la représentation des travailleurs ;

- informez les travailleurs des règles et conditions à respecter pour le contrôle ou la surveillance ;

- définissez dans un document écrit la politique d'accès aux données de communication électroniques des travailleurs, par exemple dans le règlement de travail.

Limitez les possibles ingérences dans la vie privée des travailleurs

- limitez les possibilités de traitements d'un employeur en ce qui concerne des informations enregistrées sur les terminaux des utilisateurs finaux (par exemple, dans une boîte de réception professionnelle "mixte" *de facto*) à ce dont il a réellement besoin ;

- réalisez le traitement de données le moins intrusif (qui offre donc le moins de possibilités d'identification des personnes concernées par le traitement d'informations les plus générales possibles) ;

- motivez toute intrusion plus conséquente dans les données à caractère personnel des travailleurs, ou d'un travailleur en particulier, par des éléments de fait ;

- responsabilisez les travailleurs pour qu'ils se conforment aux règles relatives à l'utilisation d'Internet et de la messagerie électronique au travail, par exemple en activant la fonction "gestionnaire d'absence du bureau" de la boîte de réception (en mentionnant les personnes à contacter) de façon à ce qu'en cas d'absence, aucune intrusion dans leur support d'informations professionnel ne soit nécessaire ;

- prenez des mesures de prévention (techniques) pour éviter les abus par les travailleurs ;

- si la prévention ne suffit pas, ne contrôlez les abus qu'au moyen de la présence d'un certain flux de courriers électroniques ou d'un comportement déterminé sur Internet, et ce selon le plan graduel prévu par la CCT n° 81 ;

- si l'existence d'un certain flux de courriers électroniques ou d'un comportement déterminé sur Internet ne suffit pas à constater l'abus, ne procédez à un contrôle que de manière exceptionnelle, par la prise de connaissance du contenu de la communication à laquelle le travailleur a participé.

Encadrez les opérations de surveillance et de contrôle

- à l'occasion d'un accès à des données de communication électroniques, que ce soit dans le cadre d'un contrôle ou non, ne traitez que des données à caractère personnel adéquates, pertinentes, exactes et actualisées. Ces données ne peuvent pas être conservées pour une durée supérieure à celle nécessaire à la réalisation de la finalité ;

- veillez à ce que la personne chargée de la recherche et de la collecte de données à caractère personnel soit une autre personne que celle qui en donne l'ordre ;

- veillez à ce que la personne chargée de la recherche agisse sur la base d'instructions les plus précises possibles, formulées par le demandeur, et qu'elle se limite, dans sa recherche, à ce qui lui a été demandé ;

- veillez à ce que la recherche se fasse autant que possible sur la base de critères pertinents qui permettent dans un premier temps d'exclure de la consultation un maximum d'informations ;

- veillez à ce que la recherche ait lieu avant tout sur la base de dates, de mots clés, de l'identité des destinataires ou des expéditeurs de messages avant d'accéder à leur contenu ;

- édictez des règles spécifiques en matière d'accès et d'utilisation pour le gestionnaire du système dans le cadre de l'exercice de sa fonction ;

- veillez à ce que les données à caractère personnel recherchées et recueillies licitement grâce à l'accès continuent à bénéficier du degré de protection initial, du fait de leur statut légal (dans le cas par exemple d'un dossier du personnel, la personne chargée de procéder à l'accès sur demande de l'employeur est tenue, après cet accès, à la même confidentialité que le collaborateur qui gère normalement le dossier du personnel) ou par le statut qui leur a été donné, à titre professionnel, par le travailleur titulaire de l'outil ou par un éventuel correspondant (par exemple, une négociation encore confidentielle avec un tiers doit donc également rester tout aussi confidentielle après l'accès) ;

- ne prenez pas de décision importante à l'encontre de la personne concernée simplement sur la base d'informations collectées dans le cadre d'un traitement de ses données à caractère personnel (par exemple dans le cadre d'une opération de surveillance ou de contrôle) ;

- avant de prendre une quelconque décision à l'encontre de la personne concernée, offrez-lui la possibilité de faire valoir son point de vue, notamment quant à l'exactitude et à la pertinence des données à caractère personnel collectées.

Garantissez le respect des règles et renforcez la sécurité de la surveillance et du contrôle

- conservez un relevé écrit de l'ensemble des opérations constituant une intrusion dans les outils informatiques ou dans les informations qu'ils génèrent (ce qui a été consulté, collecté et transmis, quand, comment, pour le compte de qui, et par qui et à qui ces informations ont été communiquées) pour permettre tout contrôle du respect, par l'employeur, du principe de finalité et du principe de proportionnalité ;

- si la gestion et la maintenance des outils et des réseaux est réalisée par un prestataire externe, veillez à ce que les règles internes d'entreprise s'appliquent également à ce prestataire et concluez un contrat de sous-traitance avec un tel prestataire ;

- soumettez l'organisation des procédures mais aussi les opérations de surveillance et de contrôle concrètement envisagées, et de manière plus générale tous les accès aux outils informatiques, si disponibles, au préposé à la protection des données de l'entreprise afin qu'il puisse en apprécier le caractère nécessaire et licite ;

- prévoyez enfin une formation en protection des données destinée à responsabiliser les personnes contrôlées et permettant de générer de bonnes pratiques dans le chef du personnel chargé de la surveillance.

177. Nous formulons encore ci-après plusieurs règles de conduite **pratiques** qui constituent des exemples ou des outils permettant de tenir compte de la LVP lors d'un accès patronal à des communications électroniques ou d'un contrôle de ces dernières concernant les problèmes rencontrés le plus fréquemment. Toutefois, les solutions suggérées ne pourront jamais être transposées aveuglément, (l'application d'une mesure déterminée peut neutraliser une autre mesure ou même impliquer une incompatibilité avec une autre mesure) et il appartient à chaque entreprise d'en évaluer la pertinence et de rechercher s'il n'existe pas d'autres solutions plus appropriées.

178. Certaines des pratiques citées relèvent plus de "tours de passe-passe" mais sont souvent des solutions efficaces pour résoudre des difficultés de respect des principes de protection de la vie privée.

Pratique n°1 : Séparer le privé du professionnel

1. Pour les informations, fichiers et documents

Exemple 1 : Stockage des informations privées

- Création sur le poste de travail d'un répertoire nommé "Privé-Nom de l'utilisateur" servant à stocker tous les documents non professionnels, répertoire ne pouvant contenir des informations professionnelles.

- Le répertoire privé est placé sur une partition du disque dur ne faisant pas l'objet de copies de sécurité (back-up) centralisées et systématiques.

Exemple 2 : Stockage des informations professionnelles

- Les informations professionnelles, à l'exclusion de toute information privée, sont obligatoirement stockées sur le disque dur d'un serveur central, le cas échéant dans des répertoires réservés à l'utilisateur. Les documents professionnels sur le poste de travail n'étant que des copies, à considérer comme temporaires et ne faisant pas nécessairement l'objet de copies de sécurité systématiques (celles-ci se faisant centralement pour les informations du serveur).

2. Pour les messages électroniques

Exemple 3 : Stockage des informations privées

- Création dans la boîte de messagerie d'un répertoire nommé "Privé-Nom de l'utilisateur" servant à stocker tous les messages non professionnels (envoyés et reçus), répertoire ne pouvant contenir des messages professionnels (les cas de non-respect pouvant faire l'objet de sanctions).

Exemple 4 : Utilisation de comptes distincts

- Attribution de deux (ou plus) comptes de messagerie avec des identifiants distincts pour chaque utilisateur, l'un pour la messagerie privée, les autres pour la messagerie professionnelle selon le type d'activité. Cette distinction peut se faire par le nom (exemple : initiales@domaine.com pour le professionnel et nom.prénom@domaine.com pour le privé) ou par le nom de domaine (par exemple : nom@domaine.com pour le professionnel et nom@domaine.net pour le privé), ou encore, via un sous-domaine du type nom@domaine.personnel.com.

3. Pour les communications Internet

Exemple 5 : Utilisation de comptes distincts

- Attribution de deux (ou plus) comptes d'utilisateurs selon le type d'activité. Une structure sémantique de l'identifiant permettant d'harmoniser les filtres de contrôle (nom0 pour le privé, nom, nom1, nom2, …pour le professionnel).

4. Par la distinction des postes de travail

Certains services ou segments d'un réseau peuvent présenter une sensibilité particulière (exemples : locaux pour la gestion des systèmes et réseaux, service des ressources humaines, …). Dans ces cas, il peut être légitime d'interdire toute activité privée sur ces postes de travail pour pouvoir les surveiller de manière stricte et permanente, tout en mettant à disposition d'autres postes de travail pour des activités moins sensibles ou privées. Une telle distinction peut aussi contribuer à l'efficacité de la séparation technique des réseaux, comme les VLAN et les VPN.

5. Par la distinction dans la signature

Les signatures structurées dans les messages peuvent aussi constituer un critère distinctif entre le professionnel et le privé.

Exemple 6 : Utilisation de signatures distinctes avec une clause de non-responsabilité standard

- L'insertion automatisée de clauses d'avertissement standard pour accompagner les messages électroniques expédiés via le serveur ou une adresse de l'entreprise : soit une déclaration ("disclaimer") précisant que le message est envoyé à titre privé et n'engage pas l'entreprise ; soit un avertissement concernant le caractère professionnel du message et la possibilité que le contenu de celui-ci fasse l'objet, sans justification nécessaire, d'une consultation ou d'une prise de connaissance par les responsables de l'entreprise.

Pratique n°2 : Exclure des activités certaines opérations dangereuses

Pour garantir le respect de certaines instructions d'utilisation des outils informatiques et éviter une surveillance qui donnerait à l'employeur accès à des informations sans utilité, il peut être opportun d'exclure certaines opérations via les outils de l'entreprise (par exemple bloquer l'accès à certains sites Internet ou bloquer certaines adresses électroniques reconnues comme dangereuses) ou de programmer des messages d'alerte destinés à l'utilisateur en cas d'opérations suspectes. Les différentes fonctions et listes de sites Internet et d'adresses à interdire sont disponibles dans les logiciels spécifiques (suites de sécurité Internet) et peuvent être complétées sur la base des besoins spécifiques de l'entreprise.

Si on compare les coûts et l'efficacité des programmes anti-virus avec ceux des suites de sécurité Internet, on peut considérer la protection anti-virus comme insuffisante face aux menaces permanentes représentées par les réseaux Internet.

Pratique n°3 : L'accès aux communications personnelles exige un encadrement spécifique

Certaines communications professionnelles peuvent avoir un caractère spécifiquement personnel (par exemple par une mention dans l'objet). L'accès à ces communications, mêmes si elles sont clairement professionnelles, ne pourra se faire qu'avec la prudence appropriée.

Exemple 1 :

- Indication "PERSONNEL" ou "CONFIDENTIEL" dans l'objet du message. Toutefois, il semble difficile d'obtenir cette discipline pour les tiers envoyant des messages à l'entreprise.

Exemple 2 :

- Utilisation de répertoires spécifiques, au sein des domaines réservés aux communications professionnelles

Exemple 3 :

- Pour sélectionner les messages et leur réserver la suite utile, on désignera une personne de confiance neutre, soumise au devoir de confidentialité et habilitée à apprécier la qualité du message. Ce n'est qu'exceptionnellement qu'un supérieur hiérarchique, un collègue ou un assistant administratif sera la personne appropriée.

Exemple 4 :

- Lorsque des informations ont un caractère sensible, les transférer dans des pièces attachées qui peuvent être protégées de manière spécifique.

Exemple 5 :

- Lorsque des personnes traitent couramment des informations de nature confidentielle (exemples : données médicales, délibéré d'un jury), ne permettre l'accès pour un contrôle qu'à des personnes habilitées à accéder à cette catégorie de données (exemple : un médecin pour les données médicales).

Pratique n°4 : Limiter la surveillance aux données nécessaires et pas de réutilisation des données collectées

Dans la mesure où l'intrusion dans l'outil de travail informatique ou de communication électronique permet facilement de collecter d'autres informations que celles (adéquates, pertinentes et non-excessives) concernées par la finalité de l'opération de surveillance, l'accès aux données, leur recherche, leur collecte et leur transmission devraient être encadrés par des procédures restrictives.

Exemples :

- Extraction, en temps réel ou dès que possible, des données de surveillance (journaux, logs, traces) pour un stockage dans une zone sécurisée ("silo" : serveur spécifique, fichier codé, …) dont les accès sont strictement limités et délimités spécifiquement.

- Précision, dans la politique de sécurité de l'information, de l'interdiction d'utiliser les informations de surveillance à toute autre fin que celles définies dans le cadre de la surveillance.

Pratique n°5 : Instaurer des incompatibilités dans les droits d'accès pour une même personne

Un utilisateur ne devrait pas pouvoir dissimuler ses actions illicites, par exemple en pouvant modifier les traces générées par ses actions. De telles limitations sont aujourd'hui possibles par le biais des outils de gestion des identités et des accès.

Pratique n°6 : Gestion des traces

Les procédures de prises de traces, de leur manipulation, de leur sauvegarde et de leur protection doivent être explicites et suffisamment précises pour créer la confiance suffisante pour une reconnaissance de recevabilité et d'opposabilité par les parties. Il n'appartient pas à la Commission de préconiser l'une ou l'autre technique mais elle suggère quelques possibilités :

Exemples :

- Création d'un fichier de cumul des traces, avant toute analyse, de manière séquentielle et incrémentale rendant toute altération ultérieure difficile, voire impossible.

- Calcul d'une empreinte avant toute analyse et sauvegardée de manière sécurisée.

- Auditabilité du respect pratique et quotidien de la bonne mise en pratique des procédures.

- En cours de traitements tracés, verrouillage permettant d'empêcher la désactivation des traces ou leur modification.

- Scellement des traces en temps réel assurant l'authenticité et l'intégrité, par l'utilisation d'outils cryptographiques appropriés.

Pratique n°7 : Définir les règles de fonctionnement dans les cas d'exception

L'utilisation normale de l'outil informatique permet d'assurer la surveillance par des règles relativement simples. Toutefois, de multiples situations d'exception occasionnent de sérieuses difficultés lorsqu'elles n'ont pas été prévues et cadrées par des règles appropriées.

1. Absence planifiée d'un travailleur

Exemples pratiques :

- Réponse automatique à l'expéditeur le prévenant de l'absence et lui indiquant la personne appropriée à laquelle le message peut être adressé s'il ne peut attendre le retour de la personne absente (principe des messages "Out of Office").

- La personne convient d'une personne de confiance habilitée à sélectionner les messages ou les fichiers professionnels en cas de nécessité justifiée et d'une urgence ne pouvant attendre le retour du travailleur.

2. Absence non planifiée ou fortuite d'un travailleur

La procédure prévue dans le cadre de la politique de sécurité de l'information ou du règlement de travail devra définir les modalités et les critères de choix de la personne de confiance habilitée à accéder aux informations du travailleur.

Exemples :

- Une personne désignée préalablement et reconnue comme "sage" est habilitée à traiter les cas délicats (exemple en milieu hospitalier : le médiateur hospitalier).

- Une personne désignée au cas par cas, en vertu d'un accord mutuel entre l'employeur et un représentant du personnel.

3. Démission ou licenciement du travailleur avec ou sans prestation du préavis

Les situations de démission ou de licenciement (pour faute grave ou non) sont toujours délicates et sources de difficultés. La procédure sera analogue à celle prévue pour l'absence non planifiée. De plus, la procédure devra préciser le sort à réserver aux messages destinés au travailleur licencié et aux fichiers professionnels et privés stockés sur son poste de travail.

Exemples pratiques :

- En cas de départ avec prestation du préavis, prévoir une procédure analogue à celle prévue pour les absences planifiées du travailleur, le cas échéant en concertation avec le travailleur au moment du départ.

- En cas de départ sans prestation du préavis, une personne est désignée au cas par cas, en vertu d'un accord mutuel entre l'employeur et un représentant du personnel ; cette personne étant habilitée à gérer les messages entrants au nom du travailleur.

- Prévoir dans la politique de sécurité de l'information la suite à réserver aux messages professionnels (transfert à un autre travailleur approprié) et aux messages privés (effacement ou transfert vers une adresse privée pendant une durée limitée d'1 mois). Il n'est pas toujours recommandé d'indiquer dans le message automatique de réponse à l'expéditeur que le travailleur ne fait plus partie du personnel de l'organisme ; une telle indication ne pourra donc se faire qu'avec le consentement explicite et formel du travailleur.

- Prévoir dans la politique de sécurité de l'information la suite à réserver aux fichiers et informations à caractère privé (les fichiers et informations professionnels pouvant être utilisés par l'employeur conformément aux règles internes).

4. Suspicion de fraude ou d'une malveillance dans le chef du travailleur

Dans ces situations délicates et difficiles aussi, l'accès se fera avec prudence et de manière "progressive", en procédant par exemple à une sélection sur les objets des messages ou d'autres critères avant de prendre connaissance du contenu.

L'Administrateur f.f., Le Président,

(sé) Patrick Van Wouwe (sé) Willem Debeuckelaere