

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

La vie privée du travailleur

Omrani, Feyrouze

Published in:
Droits de la personnalité

Publication date:
2013

Document Version
le PDF de l'éditeur

[Link to publication](#)

Citation for pulished version (HARVARD):

Omrani, F 2013, La vie privée du travailleur: questions choisies, regard critique. dans *Droits de la personnalité*. Recyclage en droit, numéro 1, Anthemis, Limal, pp. 99-148.

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

La vie privée du travailleur : questions choisies, regard critique

Feyrouze OMRANI¹

Avocate au barreau de Bruxelles
Chercheuse au Centre de Recherche Information, Droit et Société
(CRIDS - Université de Namur)

Introduction

1. La notion de vie privée a connu une intéressante évolution. Ainsi, si initialement elle visait le jardin secret de Montaigne, la sphère privée n'est plus cantonnée au domicile (lequel présente la caractéristique d'être un lieu unique, permanent, mais aussi à l'abri des regards). Aujourd'hui, la sphère privée se conçoit aussi dans une pluralité de lieux, accessibles au public ou non.

Parallèlement à cette évolution *ratione loci*, l'observateur constate aussi une évolution *ratione materie* puisque la vie privée n'est plus circonscrite aux *activités domestiques*², avec en premier plan la vie familiale et la correspondance. Elle comprend désormais des activités réalisées en dehors de la maison, en ce compris sur le lieu de travail de l'individu.

2. Dans le cadre de la protection des données et du respect de la vie privée, il n'y a pas lieu de distinguer un espace qui serait « privé » d'un espace qui serait « public ». La Cour européenne des droits de l'homme a rappelé à maintes reprises que la vie privée ne saurait se limiter au cercle intime mais, au contraire, comprend :

« [D]ans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables. Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur. Un fait, souligné par la Commission, le confirme :

¹ Cette publication s'inscrit dans le projet de recherche ELIS-IT (Expertise Localization from Informal Sources & Information Technologies) financé par la Région wallonne dans le cadre du programme WIST 3.0 qui met les technologies de l'information au service de l'économie wallonne et du développement durable. Les vues exprimées dans cette contribution relèvent de la responsabilité de son seul auteur et ne reflètent pas nécessairement la position du CRIDS.

² Rappelons que « *domo* » en latin signifie « demeure ».

dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort. Spécialement, les tâches d'un membre d'une profession libérale peuvent constituer un élément de sa vie à un si haut degré que l'on ne saurait dire en quelle qualité il agit à un moment donné.³

3. À cela s'ajoute que les technologies ont pour effet d'obscurcir la démarcation, la distinction traditionnelle entre, d'une part, la vie dite privée et, d'autre part, la vie dite professionnelle. Aujourd'hui, le travail est exécuté en tout lieu et à toute heure. Oubliées donc les limites liées au lieu unique qu'est le bureau ou encore à l'horaire de travail convenu. Le travail à domicile⁴ ne constitue plus une exception marginale et l'utilisation des *smartphones* est largement répandue. Si beaucoup de travailleurs consultent leurs courriels professionnels depuis leur lieu de villégiature, ils sont plus nombreux encore à communiquer avec leur entourage – par téléphone ou par courriel – depuis leur bureau, le cas échéant grâce aux outils mis à leur disposition par l'employeur. En somme, si le travail s'invite à la maison, la réciprocité est tout aussi vraie.

4. La présente contribution a pour objet d'examiner la vie privée du travailleur. La première partie est consacrée à l'examen critique du cadre juridique tandis que la seconde examine des questions spécifiques comme celles relatives au consentement du travailleur, à l'usage et à la surveillance de certains outils de communication tels que la téléphonie et les correspondances.

Section 1

Le cadre juridique

§ 1. Le cadre juridique est pléthorique - panorama

5. La vie privée au travail fait l'objet de normes nationales, européennes, supranationales et internationales. À ces différents niveaux de normes, s'ajoute la difficulté supplémentaire que le sujet intéresse au moins trois domaines distincts, à savoir, d'une part, la vie privée et le traitement des données à caractère personnel, d'autre part, l'usage des technologies et, en particulier, des communications électroniques, mais aussi celui de la relation de travail.

³ Cour eur. D.H., *Niemietz c. Allemagne*, 16 décembre 1992, série A, n° 251, § 29.

⁴ Voy. à ce sujet N. LEFEVER, « Exécution du contrat de travail à distance : le télétravail » in *Le droit du travail. L'ère numérique*, sous la direction de K. Rosier, Limal, Anthémis, CRIDS, 2011, pp. 121-149.

A. L'incidence de la vie privée et le traitement des données à caractère personnel⁵

6. Le cadre juridique du respect de la vie privée et des données à caractère personnel est pléthorique. Au niveau international, tout d'abord, on relève des dispositions issues de la Convention européenne des droits de l'homme (article 8), du Pacte international relatif aux droits civils et politiques (article 17), de la Déclaration universelle des droits de l'homme (article 12), de la convention n° 108 du Conseil de l'Europe.

7. Au niveau de l'Union européenne, on retient, en particulier, la directive 95/46 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 (ci-après, « la directive 95/46 »). En marge de la directive 95/46 coexiste une législation plus spécifique instaurée par le règlement 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (ci-après, « le règlement 45/2001 »)⁶. Il faut, en outre, tenir compte de la directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (ci-après, « la directive 2002/58 »), mais aussi de la charte européenne des droits fondamentaux (articles 7 et 8)⁷.

8. Au niveau national, enfin, outre l'article 22 de la Constitution, le siège de la matière réside dans 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 loi vie privée ») et dans ses arrêtés d'exécution⁸.

Pour une meilleure compréhension, rappelons brièvement ici l'articulation de la loi vie privée. Celle-ci stipule, en son article 4, les conditions *minima* requises pour qu'un traitement soit légitime. Il s'agit, pour l'essentiel, de la *qualité du traitement* (qui doit être loyal et licite), de la *qualité des données* (qui doivent être adéquates, pertinentes, non excessives, exactes, et, si nécessaire, mises à jour), de la *qualité de la finalité* (qui doit être déterminée, explicite et légitime). Pour être valable, le traitement doit, en outre, intervenir dans une des hypothèses de légitimation visée à l'article 5 de la loi vie privée. Il peut s'agir, notamment, du

⁵ Les normes mentionnées dans cette section font l'objet d'un examen détaillé dans le présent ouvrage. Voy. *supra* la contribution de J.-M. Van Gyseghem, pp. 9-46. Voy. également *infra*, § 72.

⁶ Notons que ce règlement – qui est peu connu du public compte tenu de sa portée juridique limitée – donne lieu à d'intéressants arrêts.

⁷ Pour être complète, il faut également mentionner la directive 2009/136 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques.

⁸ Notamment, l'arrêté royal du 13 février 2001 portant exécution de la loi vie privée.

consentement de la personne concernée (article 5, a)⁹, de la nécessité d'exécuter le contrat (l'article 5, b), de la nécessité pour le responsable du traitement de respecter une obligation légale à laquelle il est astreint (article 5, c), mais aussi de la nécessité de réaliser pour le responsable du traitement un intérêt légitime (article 5, f)¹⁰.

9. Ce tableau n'est cependant pas encore complet puisqu'à ces normes juridiques, il faut encore ajouter, d'une part, la jurisprudence abondante de la Cour européenne des droits de l'homme, de la Cour de justice de l'Union européenne, des juridictions nationales et, d'autre part, les avis du groupe 29¹¹, mais aussi ceux des autorités nationales de contrôle et, s'agissant de la Belgique, de la Commission de la protection de la vie privée (ci-après, « la C.P.V.P. »)¹².

B. L'usage des technologies

1) L'article 314bis du Code pénal – pendant la transmission

10. Une disposition essentielle est assurément l'article 314bis du Code pénal qui porte sur les communications électroniques et les télécommunications. Son paragraphe premier se lit comme suit :

« § 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 »¹³.

Cette disposition sanctionne donc le comportement intentionnel (et non fortuit) – *première condition* – qui consiste en l'écoute, la prise de connaissance ou l'enregistrement d'une communication privée par un tiers à cette communication – *seconde condition* – et sans que ce tiers n'ait obtenu le consentement de toutes les parties – *troisième condition*. Les conditions requises pour l'application de cette disposition sont rarement réunies dans la mesure où le comportement

est infractionnel uniquement pendant la transmission de la communication – *quatrième condition*. Les travaux préparatoires de la loi précisent que l'expression « pendant la transmission » vise « le trajet entre l'émetteur et le récepteur »¹⁴. Avec K. Rosier, il faut convenir que l'article 314bis, § 1^{er}, du Code pénal a une « pertinence limitée dès lors que les contrôles interviennent généralement postérieurement à la transmission »¹⁵. Notons que le fait de disposer du matériel qui rend possible la prise de connaissance est également réprimé¹⁶.

11. L'article 314bis, paragraphe 2, premier alinéa, a, quant à lui, une portée plus large puisqu'il sanctionne tout usage intentionnel d'une information résultant d'une communication électronique dont on prend connaissance de manière illégale en ces termes :

« § 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 ».

Il nous paraît que le caractère illégal de la prise de connaissance de la communication résulte de toute méconnaissance d'une norme légale, et notamment de toute violation des dispositions de la loi vie privée ou de la loi relative aux communications électroniques.

12. Le second paragraphe, alinéa 2 de l'article 314bis retient également notre attention¹⁷. En effet, cette disposition sanctionne le fait d'utiliser un enregistrement « légalement effectué » lorsque cette utilisation procède soit d'une intention frauduleuse soit d'un dessein de nuire. Ce qui surprend, c'est que, le plus souvent, l'intention frauduleuse et le dessein de nuire constituent soit une circonstance aggravante d'une infraction pénale soit une condition supplémentaire à un comportement déjà répréhensible.

¹⁴ Ann. Parl. Sénat, 1992-1993, n° 843/1, p. 6, www.senate.be.

¹⁵ K. ROSIER, « Chronique de jurisprudence (2002-2009) - Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », R.D.T.L., n° 35, p. 128, § 210.

¹⁶ L'article 314bis, § 2, punit « d'un emprisonnement de six mois à un an et d'une amende de deux cents euros à dix mille euros ou d'une de ces peines seulement, celui qui, indûment, possède, produit, vend, obtient en vue de son utilisation, importe, diffuse ou met à disposition sous une autre forme un dispositif, y compris des données informatiques, principalement conçu ou adapté pour permettre la commission de l'infraction prévue au § 1^{er} ».

¹⁷ Cette disposition se lit comme suit : « 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 ».

⁹ La question du consentement de la personne concernée fait l'objet de la section 2 – voy. *infra*, §§ 57 et s. Voy. *infra*, § 72.

¹¹ Le groupe 29 est le groupe de protection des personnes à l'égard du traitement des données à caractère personnel institué par l'article 29 de la directive 95/46.

¹² La C.P.V.P. est instituée par l'article 23 de la loi vie privée.

¹³ Nous soulignons.

13. La volonté du législateur est manifestement de dissuader les contrevenants puisqu'il a prévu de réprimer les tentatives de commettre des infractions visées aux paragraphes 1^{er}, 2 ou 2bis de l'article 314bis du Code pénal comme les infractions elles-mêmes¹⁸. De même, une aggravation des peines est prévue en cas de récidive¹⁹.

2) La loi relative aux communications électroniques du 13 juin 2005

a. L'interdiction de principe de l'article 124

14. La loi du 13 juin 2005 relative aux communications électroniques (ci-après, « la loi relative aux communications électroniques ») transpose en droit belge la directive 2002/58.

Ce qui est frappant, c'est que la loi relative aux communications électroniques ne définit pas la notion de « communication » ni même celle de « courrier électronique ». La directive 2002/58 qu'elle transpose le fait pourtant en ces termes :

« communication » : toute information échangée ou acheminée entre un nombre fini de parties au moyen d'un service de communications électroniques accessible au public. Cela ne comprend pas les informations qui sont acheminées dans le cadre d'un service de radiodiffusion au public par l'intermédiaire d'un réseau de communications électroniques, sauf dans la mesure où un lien peut être établi entre l'information et l'abonné ou utilisateur identifiable qui la reçoit »²⁰; et

« courrier électronique » : tout message sous forme de texte, de voix, de son ou d'image envoyé par un réseau public de communications qui peut être stocké dans le réseau ou dans l'équipement terminal du destinataire jusqu'à ce que ce dernier le récupère »²¹.

En droit belge, une seule définition est formulée à cet égard à l'article 2, 5°, de la loi relative aux communications électroniques qui définit la notion de « service de communications électroniques » comme suit :

« le service fourni normalement contre rémunération qui consiste entièrement ou principalement en la transmission, *en ce compris les opérations*

de commutation et de routage, de signaux sur des réseaux de communications électroniques,

à l'exception (a) des services consistant à fournir un contenu à l'aide de réseaux et de services de communications électroniques ou à exercer une responsabilité éditoriale sur ce contenu,

à l'exception (b) des services de la société de l'information tels que définis à l'article 2 de la loi du 11 mars 2003 sur certains aspects juridiques des services de la société de l'information qui ne consistent pas entièrement ou principalement en la transmission de signaux sur des réseaux de communications électroniques et

à l'exception (c) des services de la radiodiffusion y compris la télévision »²².

Un autre concept retient notre attention pour la suite du raisonnement, à savoir les données de trafic. L'article 2, 6°, de la loi précitée en donne la définition suivante : « toute donnée traitée en vue de l'acheminement d'une communication par un réseau de communications électroniques ou de la facturation de ce type de communication ».

15. Dans le cadre de cette contribution, les dispositions les plus pertinentes de la loi relative aux communications électroniques en sont les articles 124 et 125. L'article 124²³ pose l'interdiction de principe de traiter le contenu d'une communication électronique, mais aussi des données de trafic et des données de localisation. L'interdiction est formulée comme suit :

« 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;

¹⁸ Conformément à l'article 314bis, § 3.

¹⁹ L'article 314bis, § 4, se lit comme suit : « Les peines prévues aux §§ 1^{er} à 3 sont doublées si une infraction à l'une de ces dispositions est commise dans les cinq ans à compter du prononcé d'un jugement ou d'un arrêt, passé en force de chose jugée, portant condamnation en raison de l'une de ces infractions ou de l'une des infractions visées à l'article 259bis, §§ 1^{er} à 3 ».

²⁰ Art. 2, d, de la directive 2002/58.

²¹ Art. 2, h, de la directive 2002/58.

²² Conformément à l'article 2, 5°, de la loi relative aux communications électroniques. Le renvoi à la ligne et le léger retrait procèdent d'un choix de présentation de l'auteur pour faciliter la lecture de cette disposition.

²³ Anciennement, article 109ter D de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques.

4° modifier, supprimer, révéler, stocker ou faire un usage quelconque de l'information, de l'identification ou des données obtenues intentionnellement ou non »²⁴.

16. La condition objective d'absence de consentement de toutes les personnes concernées n'est pas sans poser de questions. En pratique, elle paraît difficile à mettre en œuvre puisque sont visées non seulement les personnes concernées directement, mais de surcroît celles qui le sont « indirectement ».

S'agissant de la première catégorie, on suppose qu'il s'agit en premier chef des parties à la communication électronique.

On est plus circonspect s'agissant de la seconde catégorie de personnes. S'agit-il des personnes mises en copie du courriel ? S'agit-il des personnes mentionnées explicitement dans le courriel ou qui y sont intéressées ? On peut supposer que ces personnes indirectement concernées peuvent ne pas avoir elles-mêmes connaissance de l'existence de la communication électronique concernée. Comment, dans ce cas, pourraient-elles consentir à la prise de connaissance de celle-ci par un tiers ? À cela s'ajoute que, sans avoir pris connaissance du contenu de la communication électronique, comment savoir à qui s'adresser pour obtenir le consentement préalable requis par l'article 124 ?

Enfin, on citera encore comme obstacle potentiel la problématique de la possibilité pour le travailleur de consentir librement compte tenu de la relation de travail. Cette question précise sera examinée à la prochaine section.

17. L'interdiction de l'article 124 de loi relative aux communications électroniques est faite à l'égard de toute personne comme le suggère l'expression « nul ne peut ». La version en langue néerlandaise de la loi conforte ce sentiment puisque l'expression retenue est « *mag niemand* »²⁵.

Serait-ce à dire que l'interdiction ne vaut pas à l'égard d'un outil informatique, tel un logiciel ? Nous le pensons. Du reste, le recours aux logiciels antis-pam n'est pas contesté. Il est question pour le logiciel d'examiner – pendant leur transmission – les communications électroniques et d'empêcher qu'elles ne

²⁴ Nous soulignons.

²⁵ La disposition se lit comme suit :

« Indien men daartoe geen toestemming heeft gekregen van alle andere, direct of indirect betrokken personen, mag niemand :

1° met opzet kennis nemen van het bestaan van informatie van alle aard die via elektronische weg is verstuurd en die niet persoonlijk voor hem bestemd is ;

2° met opzet de personen identificeren die bij de verzending van de informatie en de inhoud ervan betrokken zijn ;

3° onverminderd de toepassing van de artikelen 122 en 123, met opzet kennis nemen van gegevens inzake elektronische communicatie en met betrekking tot een andere persoon ;

4° de informatie, identificatie of gegevens die met of zonder opzet werden verkregen, wijzigen, schrappen, kenbaar maken, opslaan of er enig gebruik van maken ».

poursuivent leur acheminement si elles constituent un *spam*. Cette interception de la communication et son blocage procèdent tout à la fois de la volonté de préserver le système informatique, mais aussi d'épargner à l'utilisateur final la réception de *pourriels*.

Le recours à des logiciels plus complexes qui suppose un *usage* de l'information obtenue par le biais du logiciel nous paraît davantage problématique. Cet usage suppose en effet qu'après avoir identifié une information paramétrée cette information fasse ultérieurement l'objet d'un traitement au sens de la loi vie privée.

18. À la question de savoir si la « connaissance de l'existence d'une information » comprend, ou non, la connaissance de l'information elle-même et, partant, la connaissance du contenu de cette communication électronique, la Cour de cassation répond par l'affirmative dans un arrêt du 1^{er} octobre 2009²⁶. À raison, elle relève que « [Q]uiconque prend connaissance du contenu d'un courriel ne peut le faire sans prendre connaissance simultanément de son existence. La prise de connaissance et l'usage du contenu d'un courriel sont liés à la prise de connaissance et à l'usage de l'existence de ce courriel ».

19. L'article 124 de la loi relative aux communications électroniques, 1° à 3°, conditionne l'interdiction au caractère intentionnel de la démarche. La prise de connaissance de la communication électronique ou l'identification des personnes concernées n'est pas interdite lorsqu'elle intervient fortuitement. Les travaux parlementaires admettaient même « une simple indiscretion »²⁷.

Cependant, la distinction du caractère fortuit ou intentionnel n'est plus retenue quand il est question de faire un usage quelconque de l'information obtenue²⁸. En somme, si un employeur prend fortuitement – et donc légalement – connaissance d'un courriel destiné à son employé, il ne pourrait pas en faire usage sans violer l'article 124, 4°, de la loi relative aux communications électroniques²⁹.

²⁶ Cass., 1^{er} octobre 2009, n° C.08.0064.N, www.cass.be. Avant le prononcé de cet arrêt, certains auteurs affirmaient que l'interdiction ne portait pas sur les données de contenu. Voy. en ce sens notamment S. VAN WASSENHOVE, « Le respect de la vie privée dans l'usage des nouvelles technologies », in *Vie privée du travailleur et prérogatives patronales*, sous la direction scientifique de J.-F. Leclercq, C.J.B., Édition du jeune barreau de Bruxelles, 2005, p. 154 et références citées.

²⁷ Ann. Parl. Sénat, 1992-1993, n° 843/1, p. 6, www.senate.be.

²⁸ Conformément à l'article 124, 4°, de la loi relative aux communications électroniques.

²⁹ Voyez cependant *infra* la jurisprudence *Antigone* développée aux §§ 42 et s.

b. Les exceptions de l'article 125

20. L'interdiction de l'article 124 de la loi relative aux communications électroniques est tempérée d'exceptions limitativement énumérées par l'article 125 de cette même loi, lequel se lit comme suit :

« § 1^{er}. Les dispositions de l'article 124 de la présente loi et les articles 259bis et 314bis du Code pénal ne sont pas applicables :

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

§ 2. Le Roi fixe, après avis de la Commission de la protection de la vie privée et de l'Institut, par arrêté délibéré en Conseil des ministres, les modalités et les moyens à mettre en œuvre en vue de permettre l'identification, le repérage, la localisation, les écoutes, la prise de connaissance et l'enregistrement des communications électroniques »³⁰.

En pratique, les exceptions à l'interdiction sont limitées à l'obligation ou l'autorisation légale, d'une part, et, d'autre part, à des exigences techniques requises pour assurer le fonctionnement du réseau et la bonne exécution du service de communication électronique.

La marge de manœuvre est assurément ténue.

c. La sanction de l'article 145

21. Notons, enfin, que la méconnaissance de l'article 124 de la loi relative aux communications électroniques est sanctionnée pénalement par l'article 145 de

cette même loi. Celle-ci prévoit, en effet, une amende de 50 à 50 000 EUR soit, en tenant compte des décimes additionnels, d'une amende de 275 EUR à 275 000 EUR.

C. L'incidence de la relation de travail

22. Il faut également tenir compte du contexte dans lequel intervient, par hypothèse, le traitement de données à caractère personnel, à savoir la relation de travail. À ce titre, la loi sur le contrat du travail du 3 juillet 1978 (ci-après, « la loi sur le contrat de travail ») occupe une place importante.

23. Conformément aux articles 2 et 3 de la loi sur le contrat de travail, les ouvriers et employés travaillent sous l'autorité de leur employeur. À cela s'ajoutent les obligations que l'article 17 de cette même loi impose au travailleur, à savoir :

- « 1° exécuter son travail avec soin, probité et conscience, au temps, au lieu et dans les conditions convenus ;
- 2° agir conformément aux ordres et aux instructions qui lui sont données par l'employeur, ses mandataires ou ses préposés, en vue de l'exécution du contrat ;
- 3° s'abstenir, tant au cours du contrat qu'après la cessation de celui-ci :
 - a) de divulguer les secrets de fabrication, ou d'affaires, ainsi que le secret de toute affaire à caractère personnel ou confidentiel dont il aurait eu connaissance dans l'exercice de son activité professionnelle ;
 - b) de se livrer ou de coopérer à tout acte de concurrence déloyale ;
- 4° s'abstenir de tout ce qui pourrait nuire, soit à sa propre sécurité, soit à celle de ses compagnons, de l'employeur ou de tiers ;
- 5° restituer en bon état à l'employeur les instruments de travail et les matières premières restées sans emploi qui lui ont été confiés ».

Le lien hiérarchique entre l'employeur et le travailleur confère au premier le droit de contrôler le second. Dans certains cas, s'agissant par exemple du respect des bonnes mœurs, cette faculté se transforme en obligation. On comprend aussi le souhait de l'employeur de contrôler la qualité du travail fourni, le respect des horaires de travail, le caractère légitime et licite de l'usage des outils de travail qu'il met à la disposition du travailleur. Il paraît légitime que l'employeur exerce en conséquence son autorité notamment par le biais d'une surveillance. Aussi l'autorité de l'employeur implique-t-elle, selon la Cour du travail de Gand dans un arrêt du 4 avril 2001, que « [L']employeur a le droit, en vertu de la loi relative aux contrats de travail, d'instaurer unilatéralement des directives

³⁰ Nous soulignons.

et obligations quant à l'informatique sans consensus ou implications des travailleurs ».³¹

24. Le contrôle des outils mis à disposition par l'employeur se justifie par l'article 16 de la loi sur le contrat de travail qui oblige l'employeur et le travailleur à respecter les convenances et les bonnes mœurs pendant l'exécution du contrat. Une obligation plus grande pèse sur l'employeur qui est, en outre, tenu d'assurer ce respect.

Le plus souvent, l'employeur – qui fournit aux travailleurs les outils nécessaires à la réalisation du travail convenu – est propriétaire de ces outils. À ce titre, conformément à l'article 544 du Code civil, il dispose donc du droit de jouir et de disposer de ces outils de manière la plus absolue sans pouvoir en faire un usage prohibé par les lois ou par les règlements.

Comme l'énonce le Tribunal du travail de Bruxelles dans un jugement du 2 mai 2000 : « En tant que propriétaire de l'outil mis à disposition du travailleur, l'employeur a le droit de déterminer les conditions d'utilisation de l'outil informatique. Toutefois, le droit de réglementer l'usage de l'outil informatique ne confère nullement à l'employeur un droit absolu de contrôle. »³²

D. Les dispositions qui touchent à la vie privée et à la relation de travail

25. À proprement parler, la loi ne régit pas la question de la vie privée au travail. Dans la pratique, la nécessité d'instrument mixte se fait sentir, ce qui explique l'existence de conventions collectives de travail à ce sujet (1), mais aussi d'avis formulés par la C.P.V.P. (2).

1) Les conventions collectives de travail

26. Selon les termes de l'article 5 de la loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions paritaires (ci-après, « la loi sur les CCT »), « la convention collective de travail est un accord conclu entre une ou plusieurs organisations de travailleurs et une ou plusieurs organisations d'employeurs ou un ou plusieurs employeurs déterminant les relations individuelles et collectives entre employeurs et travailleurs au sein d'entreprises ou d'une branche d'activité et réglant les droits et obligations des parties contractantes ». Ces conventions peuvent être rendues obligatoires par le Roi, conformément à l'article 28 de la loi sur les CCT. La convention rendue obligatoire ne s'applique cependant pas à tous les travailleurs et employeurs.

³¹ C. trav. Gand, 4 avril 2001, J.T.T., 2002, p. 49.

³² Trib. trav. Bruxelles, 2 mai 2000, *Computerr*, 2001, p. 26, note D. CASAER.

D'une part, en sont en toute hypothèse exclus les travailleurs visés à l'article 2, § 3, de la loi sur les CCT, à savoir :

- les personnes occupées par l'État, les Communautés, les Régions, les Commissions communautaires, les provinces, les communes, les établissements publics qui en dépendent et les organismes d'intérêt public à l'exception de la Société fédérale de Participations et d'Investissement, de l'Autorité des services et marchés financiers, du Fonds de participation, de l'Office national du Ducroire, de la Banque nationale de Belgique, de la S.A. CREDIBE, de la S.A. Loterie nationale, de la « Vlaamse Instelling voor Technologisch Onderzoek », des sociétés de logement social agréées conformément aux codes du logement des Régions et des sociétés anonymes de droit public « Brussels South Charleroi Airport- Security » et « Liège-Airport-Security » ;
- les personnes occupées dans des centres de formation professionnelle en application de la législation relative à l'emploi ou à la formation professionnelle des demandeurs d'emploi ;
- les membres du personnel subventionnés par l'État occupés par les établissements d'enseignement libre subventionnés ; et
- les travailleurs engagés dans le cadre d'un contrat de travail ALE.

L'exclusion concerne essentiellement les travailleurs du secteur public³³.

D'autre part, seuls les employeurs et travailleurs qui relèvent de l'organe paritaire conformément à l'article 31 de la loi sur les CCT.

27. Trois conventions collectives du travail retiennent plus particulièrement notre attention. Il s'agit de :

- la convention collective de travail n° 68, conclue le 16 juin 1998 au sein du Conseil national du travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail rendue obligatoire par l'arrêté royal du 20 septembre 1998 (ci-après, « la CCT n° 68 ») ;
- la convention collective de travail n° 81 du 26 avril 2002, conclue au sein du Conseil national du travail, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communications électroniques en réseau rendue obligatoire par l'arrêté royal du 12 juin 2002 (ci-après, « la CCT n° 81 ») ; et
- la convention collective de travail n° 89 du 30 janvier 2007, conclue au sein du Conseil national du travail, concernant la prévention des vols et les

³³ Voy. en ce sens S. GILSON, F. LAMBINET, K. ROSIER, « Le droit au respect de la vie privée du travailleur. État des lieux », *Limal, Anthemis, CRIDS*, 2012, p. 13, § 10.

contrôles de sortie des travailleurs quittant l'entreprise ou le lieu de travail rendue obligatoire par l'arrêté royal du 25 avril 2007 (ci-après, « la CCT n° 89 »).

28. De ces trois conventions, seule la CCT n° 81 sera examinée ultérieurement à l'occasion de l'examen des certains outils de communication. Relevons déjà que l'objectif poursuivi par ces conventions est de trouver un équilibre entre les droits légitimes des travailleurs et des employeurs puisque, selon l'article 3 de la CCT n° 81 :

- « - les travailleurs reconnaissent le principe selon lequel l'employeur dispose d'un droit de contrôle sur l'outil de travail et sur l'utilisation de cet outil par le travailleur dans le cadre de l'exécution de ses obligations contractuelles, y compris lorsque cette utilisation relève de la sphère privée, compte tenu des modalités d'application prévues par la présente convention ;
- les employeurs respectent le droit des travailleurs à la protection de leur vie privée dans le cadre de la relation de travail et des droits et obligations que celle-ci implique pour chacune des parties ».

2) Les avis et recommandations de la C.P.V.P.

29. La C.P.V.P.³⁴ s'est prononcée à maintes reprises sur la problématique du contrôle que l'employeur exerce sur l'utilisation de la messagerie électronique et de l'internet par son personnel, notamment, à l'occasion de :

- 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'in-

³⁴ Notons que tous les avis de la C.P.V.P. sont accessibles au départ de son site web : <http://www.privacycommission.be>.

ternet 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, P.M.E., Classes moyennes et Énergie.

30. Deux documents récents retiennent notre attention dès lors qu'ils abordent la question des communications électroniques, à savoir, d'une part, l'avis d'initiative n° 10/2000 du 3 avril 2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail (ci-après, « l'avis n° 10/2000 ») (a) et, d'autre part, la recommandation d'initiative n° 08/2012 du 2 mai 2012 relative au contrôle de l'employeur quant à l'utilisation des outils de communications électroniques sur le lieu de travail (ci-après, « la recommandation n° 08/2012 ») (b). L'enseignement de ceux-ci est résumé ci-après.

a. L'avis n° 10/2000 du 3 avril 2000 – Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail

31. La C.P.V.P. rappelle les exigences relatives à la transparence, à la proportionnalité et la nécessité, à la durée de conservation des données et celle relative à la sécurité. En particulier, elle insiste, au nom de l'exigence de transparence, sur la nécessité d'un dialogue entre l'employeur et les employés au sujet de la politique de contrôle de l'employeur. Cette politique doit, par ailleurs, énoncer de manière suffisamment détaillée :

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

- le droit d'accès de l'employé aux données à caractère personnel le concernant »³⁵.

S'agissant du secteur privé, les méthodes de contrôle doivent, en outre, être concertées avec les employés et leurs représentants.

32. L'exigence de proportionnalité et de nécessité conduit, en outre, la C.P.V.P. à considérer que : « Tout contrôle devrait être ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail. Un contrôle général et *a priori* de l'ensemble des données de télécommunication de même qu'un enregistrement systématique de l'ensemble de ces données apparaît disproportionné par rapport à l'objectif poursuivi »³⁶.

b. La recommandation 8/2012 du 2 mai 2012 – Recommandation d'initiative relative au contrôle de l'employeur quant à l'utilisation des outils de communication électronique sur le lieu de travail

33. La portée de la recommandation n° 08/2012 est limitée à l'utilisation de la messagerie électronique et d'internet au départ de l'ordinateur de bureau mis à disposition par l'employeur³⁷. Sont donc exclus de la recommandation les usages au départ de l'ordinateur portable appartenant à l'employeur, mais aussi les autres outils de communication tels que les communications téléphoniques, les SMS ou encore la géolocalisation³⁸. En revanche, la recommandation examine tant les données de trafic que les données de contenu.

34. À l'occasion de cette recommandation, la C.P.V.P. formule des bonnes pratiques, de bons sens. Elle appelle, notamment, à :

- l'exclusion de certaines opérations dangereuses des activités professionnelles ;
- la mise en place d'un encadrement spécifique pour les communications personnelles ;
- la limitation de la surveillance aux données nécessaires ;
- l'interdiction de réutiliser des données collectées ;
- la gestion des différents profils en ce compris l'instauration d'incompatibilités ;
- la gestion des traces, des logs, etc. ;
- la définition des règles de fonctionnement dans les cas d'exception.

³⁵ Voy. page 5 de l'avis 10/2000.

³⁶ Voy. page 6 de l'avis 10/2000.

³⁷ Page 5, § 13, de la recommandation n° 08/2012.

³⁸ Page 5, § 12, de la recommandation n° 08/2012.

35. Au niveau européen, on mentionne l'adoption par le Groupe 29 d'un document de travail concernant également la surveillance des communications électroniques sur le lieu du travail³⁹.

§ 2. L'absence de régime légal spécifique et clair

A. Le pragmatisme

36. Il résulte du régime légal en place, *de facto*, une interdiction de contrôle par les employeurs quant à l'utilisation par les travailleurs des outils de communication électronique. Ceci est problématique et explique le nombre important de demandes adressées à la C.P.V.P. sur ce point, mais aussi la volonté des partenaires sociaux d'assouplir le système en place. Tous cherchent une solution qui soit à la fois respectueuse du droit des travailleurs au respect de leur vie privée et de l'intérêt légitime de l'employeur d'assurer le bon fonctionnement de son entreprise.

Cette situation est qualifiée par la C.P.V.P. de « problème complexe et récurrent qui reste d'actualité »⁴⁰. La C.P.V.P. entend apporter une réponse pratique et pragmatique au problème qu'elle identifie. Le Conseil national du travail ne dit pas autre chose puisqu'il reconnaît la nécessité d'aménager les normes juridiques existantes⁴¹.

À la question de savoir si « [L]e travailleur [peut] invoquer la loi vie privée ou d'autres dispositions légales pour empêcher l'employeur d'accéder à cette information, par exemple pour contrôler la qualité de son travail et empêcher toute surveillance et tout contrôle exact qu'il pose via les outils mis à sa disposition⁴² », il faut répondre par l'affirmative, tout en apportant quelques nuances – en ce compris celles qui résultent de l'abus de droit. C'est donc surprenant que la commission chargée de veiller au respect de la vie privée affirme « la réponse à cette question reste controversée ». En réalité, la réponse n'est pas controversée *de lege lata*, mais uniquement contestable *de lege ferenda*.

³⁹ Groupe 29, W.P. n° 55 du 29 mai 2002, n° 5401/01.

⁴⁰ Voy. page 3 de la recommandation n° 08/2012.

⁴¹ Voy. en ce sens le préambule de la CCT n° 81 et notamment : « Au terme de leur analyse, les organisations de travailleurs et d'employeurs représentées au sein du Conseil national du travail ont estimé que conclure une convention collective de travail était utile dès lors qu'elle permettrait 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. Il faut cependant admettre des aménagements, mais stricts quant à leur mise en œuvre sur le lieu de travail. Ces aménagements tiennent au caractère professionnel ou privé du contenu des données de communication électroniques en réseau, l'attribution d'un caractère professionnel ou privé à l'ensemble des données de communication électroniques en réseau ne pouvant toutefois aboutir à rendre la convention collective de travail inopérante dans les garanties qu'elle offre tant aux employeurs qu'aux travailleurs ».

⁴² Voy. page 4, § 8, de la recommandation n° 08/2012.

B. Les constats d'illégalité et d'inconstitutionnalité – conséquences

37. Il apparaît des développements *supra* que le cadre juridique est assurément difficile à appréhender compte tenu du nombre élevé des normes susceptibles de s'appliquer à la question de la vie privée au travail. À cette difficulté quantitative s'ajoute, de surcroît, une difficulté qualitative résultant du caractère contradictoire des règles qui traitent de cette question.

En effet, certaines dispositions des conventions collectives de travail permettent, nous l'avons vu, des comportements que la loi vie privée prohibe ou, à tout le moins, entoure de garanties procédurales. C'est précisément l'objectif qui est poursuivi puisque le souhait est d'assouplir le cadre juridique strict et, partant, d'y déroger⁴³.

38. On rappellera utilement que les positions que la C.P.V.P. prend à l'occasion de ses avis et recommandations n'ont pas force de loi et ne revêtent même aucun caractère obligatoire⁴⁴. Toute dérogation à la loi que ces avis et recommandations impliquent se fait en dehors de toute justification en droit positif.

1) Les dérogations sont illégales (et nulles)

39. Les CCT n° 68, CCT n° 81 et CCT n° 89 dérogent à la loi vie privée, à la loi relative aux communications électroniques et à l'article 314bis du Code pénal. Ces dispositions sont, à tout le moins, des dispositions impératives compte tenu de la sanction pénale dont la méconnaissance est assortie. Selon le professeur Van Ommeslaghe, elles seraient même d'ordre public puisqu'elles touchent à un droit fondamental de l'homme. Or, conformément à l'article 51, 1°, de la loi sur les CCT, dans la hiérarchie des sources des obligations dans les relations de travail entre employeurs et travailleurs, la loi dans ses dispositions impératives prime sur les conventions collectives du travail. Mieux, l'article 9 de la loi sur les CCT, sanctionne par la nullité « les dispositions d'une convention [...] contraires aux dispositions impératives des lois et arrêtés, des traités et règlements internationaux obligatoires en Belgique ».

Ces dérogations sont non seulement nulles aux termes de l'article 9 de la loi précitée, mais de surcroît inopérantes en application de l'article 51 de cette même loi.

2) Les dérogations sont inconstitutionnelles

40. Le caractère contradictoire des règles est aussi une particularité du droit belge dans la mesure où la législation belge est plus contraignante – plus protectrice – que la législation européenne. Ainsi, les conditions requises par la loi relative aux communications électroniques sont-elles plus strictes que celles de la directive 2002/58 qu'elle transpose. De même, si la Cour européenne⁴⁵ a une conception large de la « loi », l'article 22 de la constitution ne tolère-t-il que des exceptions prévues par la loi au sens formel du terme⁴⁶. Cette exigence constitutionnelle a, du reste, été rappelée à l'occasion d'un arrêt prononcé par la Cour d'arbitrage le 19 juillet 2005⁴⁷.

41. Avec Pierre Joassart, il faut convenir que les conventions collectives ne rentrent pas dans la définition constitutionnelle de la loi et conclure, en conséquence, à leur inconstitutionnalité respective⁴⁸. En d'autres termes, les CCT n° 68, n° 81 et n° 89 ne peuvent pas justifier une ingérence au droit au respect de la vie privée de chacun.

⁴⁵ Voy. notamment Cour eur. D.H., *Sunday Times c. Royaume-Uni*, 26 avril 1979, *Public. Cour eur. D.H.*, série A, n° 6538/74, recueil vol. 30, p. 31 (accessible en lien direct : <http://hudoc.echr.coe.int/sites/fra/pages/search.aspx?i=001-62140>) : « Aux yeux de la Cour, les deux conditions suivantes comptent parmi celles qui se dégagent des mots "prévues par la loi". Il faut d'abord que la "loi" soit suffisamment accessible : le citoyen doit pouvoir disposer de renseignements suffisants, dans les circonstances de la cause, sur les normes juridiques applicables à un cas donné. En second lieu, on ne peut considérer comme une "loi" qu'une norme énoncée avec assez de précision pour permettre au citoyen de régler sa conduite; en s'entourant au besoin de conseils éclairés, il doit être à même de prévoir, à un degré raisonnable dans les circonstances de la cause, les conséquences de nature à dériver d'un acte déterminé. Elles n'ont pas besoin d'être prévisibles avec une certitude absolue : l'expérience la révèle hors d'atteinte. En outre la certitude, bien que hautement souhaitable, s'accompagne parfois d'une rigidité excessive; or le droit doit savoir s'adapter aux changements de situation. Aussi beaucoup de lois se servent-elles, par la force des choses, de formules plus ou moins vagues dont l'interprétation et l'application dépendent de la pratique ».

⁴⁶ L'article 22 de la Constitution se lit en effet comme suit : « 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 ».

⁴⁷ C.A., 19 juillet 2005 n° 131/2005, M.B., 8 août 2005, pp. 34459-34462. Il s'agit d'un recours en annulation à l'encontre de l'article 57, § 2, alinéa 1°, 2°, et alinéa 2, de la loi du 8 juillet 1976 organique des centres publics d'action sociale, telle qu'elle a été modifiée par l'article 483 de la loi-programme du 22 décembre 2003, introduit par l'a.s.b.l. « Défense des Enfants - International - Belgique - Branche francophone (D.E.I. Belgique) » et autres. Cet arrêt est disponible en lien direct : <http://www.const-court.be/public/f/2005/2005-131f.pdf>. § B.5.2. « Bien que, en utilisant le terme "loi", l'article 8.2 de la Convention européenne précitée n'exige pas que l'ingérence qu'il permet soit prévue par une "loi", au sens formel du terme, le même mot "loi" utilisé à l'article 22 de la Constitution désigne une disposition législative. Cette exigence constitutionnelle s'impose au législateur belge, en vertu de l'article 53 de la Convention européenne, selon lequel les dispositions de la Convention ne peuvent être interprétées comme limitant ou portant atteinte aux droits de l'homme et aux libertés fondamentales reconnues notamment par le droit interne ».

⁴⁸ P. JOASSART, « Le droit à la vie privée dans les relations de travail : quelques conclusions », in *La vie privée au travail*, Limal, Anthemis, 2011, p. 153. Voy. également en ce sens J.-Fr. NEVEN, « Les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, sous la direction scientifique de J.-F. LECLERCQ, C.J.B., Édition du jeune barreau de Bruxelles, 2005, p. 35, n° 25 et références citées; P. DE HERT, O. DE SCHUTTER et B. SMEESTERS, « Emploi, vie privée et technologies de surveillances », J.T.T., 2001, p. 9 et G. DEMEZ, *Protection de la vie privée et nouvelles technologies*, CUP, 2002, vol. 56, pp. 319-321.

⁴³ Voy. *supra*, § 36.

⁴⁴ Voy. en ce sens notamment Trib. trav. Gand, 4 avril 2001, J.T.T., 3/2002, pp. 49-52.

C. La solution jurisprudentielle par le biais du droit de la preuve⁴⁹

42. Le droit positif instaure un régime de protection de la vie privée excessif puisque le législateur reste en défaut d'adopter des dérogations nécessaires dans la relation de travail. En l'absence de dérogation, la loi vie privée apparaît parfois comme une loi scléreuse puisqu'elle prive l'employeur de moyens d'action.

La seule marge de manœuvre de l'employeur résulte de la combinaison de deux éléments. Le premier est – hormis les hypothèses de violation grave et caractérisée – l'absence en pratique de conséquences d'une méconnaissance des dispositions protectrices de la vie privée. Cette impunité de fait s'explique par le fait que la législation est méconnue et rarement invoquée devant les tribunaux. Du reste, il arrive aussi que les magistrats soit ne connaissent pas la loi soit ne perçoivent pas le caractère fondamental du droit au respect de la vie privée. À cela s'ajoute qu'il ne s'agit manifestement pas d'une priorité dans le cadre de la politique de répression des parquets. Le second élément résulte d'une évolution jurisprudentielle aux termes de laquelle la Cour de cassation a admis la production d'éléments de preuve obtenus irrégulièrement remettant en cause sa jurisprudence constante de l'exclusion de la preuve irrégulière ou illégale⁵⁰.

1) La jurisprudence de la Cour de cassation : une preuve illicite mais admissible

43. Le premier arrêt à mentionner est celui prononcé le 27 février 2001⁵¹ par la deuxième chambre de la Cour de cassation en manière pénale. Dans cette affaire, le demandeur en cassation faisait grief au juge d'appel d'avoir violé l'article 8, alinéa 1^{er}, de la CEDH en admettant l'ingérence par un employeur dans la vie privée de son employé et les conséquences de celle-ci dans le cadre de poursuites pénales. En l'espèce, l'employeur avait fait usage d'un système de vidéosurveillance pour constater le vol de son employé à ses dépens. La vidéo a été remise à la police dans le cadre d'une plainte déposée par l'employeur. L'employé entendait conclure au caractère illégal de la vidéosurveillance (et donc de la preuve) compte tenu de la violation de la vie privée dont elle résulte. Après avoir rappelé que le droit au respect de la vie privée tel que consacré par la CEDH n'est pas absolu, la Cour de cassation énonce que : « Cette dis-

position conventionnelle n'empêche pas que, sur la base d'une présomption légitime de l'implication de son employé dans des infractions commises à son détriment, un employeur prenne des mesures afin de prévenir ou de constater de nouveaux faits punissables au moyen de vidéosurveillance dans un espace accessible au public du magasin qu'il exploite ; que, pour autant qu'elle a pour objectif la dénonciation des faits aux autorités et, partant de cet objectif, qu'elle est adéquate, utile et non excessive, une telle mesure n'implique pas d'ingérence dans l'exercice de ce droit au sens de l'article 8, alinéa 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales ; que l'article 8, alinéa 2, de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales n'implique pas que la mesure ainsi prise doit être préalablement annoncée. »

Cet arrêt est naturellement intéressant, mais sa portée reste limitée puisque l'examen de la Cour de cassation se fait à la seule lumière de la CEDH. Or, nous avons mis en lumière *supra* au paragraphe 40 que le droit positif belge est plus protecteur que le droit européen, notamment eu égard à la nécessité d'une loi – au sens formel – pour déroger à l'article 22 de la Constitution. En l'espèce, la Cour de cassation ne s'est donc pas prononcée sur une conséquence de la violation de la loi vie privée ou encore de la violation de l'article 314bis du Code pénal⁵².

44. À l'occasion de l'arrêt du 14 octobre 2003⁵³, dit arrêt *Antigone*, la seconde chambre de la Cour de cassation poursuit la révolution commencée deux ans plus tôt puisque, comme le résume K. Rosier, « la prise en compte des preuves illicites devient [...] la règle et leur écartement l'exception »⁵⁴. Désormais, le principe est la faculté pour le magistrat, lorsqu'il forme sa conviction, de prendre en considération un élément de preuve obtenu irrégulièrement. Il n'est privé de cette faculté que dans trois hypothèses limitativement énumérées, à savoir, d'une part, lorsque le respect de certaines conditions de forme est prescrit à peine de nullité ; lorsque l'irrégularité commise a entaché la fiabilité de la preuve, d'autre part ; et, enfin, lorsque l'usage de la preuve est contraire au droit à un procès équitable.

45. La seconde chambre de la Cour de cassation a confirmé la jurisprudence *Antigone* à l'occasion de l'arrêt du 2 mars 2005, dit arrêt *Manon*⁵⁵ et a précisé deux éléments.

⁴⁹ Pour plus de développements, voy. à ce sujet F. KEFER, « La légalité de la preuve confrontée au droit à la vie privée du salarié », in *La vie privée au travail*, sous la direction de M. Verdussen et P. Joossart, Anthemis, 2011, pp. 17-58 ; K. ROSIER, « La preuve irrégulière : quand *Antigone* ouvre la boîte de Pandore. Commentaire de l'arrêt *Lee Davies* rendu par la Cour européenne des droits de l'homme le 28 juillet 2009 », *Chr. D.S. – Soc. Kron.*, 2010, n° 06, pp. 289-292 ; T. LÉONARD et K. ROSIER, « La jurisprudence *Antigone* face à la protection des données : salvatrice ou dangereuse ? », *R.D.T.L.*, n° 36/2009, pp. 5-10.

⁵⁰ Cass., 12 mars 1923, *Pas.*, 1923, I, pp. 233 et 234.

⁵¹ Cass. (2^e ch.), 27 février 2001, n° P99.0706.N/1, www.cass.be, lien direct : http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20010227-8.

⁵² Ces moyens ont été invoqués devant la Cour de cassation sans avoir été antérieurement invoqués devant les juridictions de fond. La Cour de cassation n'avait d'autre choix que de les rejeter pour ce motif.

⁵³ Cass. (2^e ch.), 14 octobre 2003, n° P030762N, www.cass.be, lien direct : http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20031014-18.

⁵⁴ K. ROSIER, « La jurisprudence *Antigone* face à la protection des données : salvatrice ou dangereuse ? », *R.D.T.L.*, n° 36/2009, p. 6, n° 2.

⁵⁵ Cass. (2^e ch.), 2 mars 2005, n° P04.1644.F, www.cass.be, lien direct : http://jure.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20050302-10.

Le premier a trait au fait que la violation par l'employeur de son obligation d'information préalable du contrôle qu'il met en place n'interdit pas nécessairement toute poursuite pénale à charge du travailleur dont l'outil a été surveillé à son insu.

Le second porte sur la proportionnalité qui doit guider le magistrat lorsqu'il entend tenir compte d'un élément de preuve obtenu illégalement. Ainsi, doit-il tenir compte de ce que la circonstance que l'illicéité commise est, ou non, sans commune mesure avec la gravité de l'infraction dont l'acte irrégulier a permis la constatation ou encore de ce que cette irrégularité est, ou non, sans incidence sur le droit ou la liberté protégés par la norme transgressée.

46. Le 12 octobre 2005⁵⁶, suite au pourvoi du procureur général de la Cour d'appel de Mons, la seconde chambre de la Cour de cassation a confirmé sa jurisprudence. En l'espèce, la Cour d'appel de Mons, chambre correctionnelle, refuse d'avoir égard aux preuves résultant d'informations communiquées par des policiers français alors qu'ils se trouvaient sur le territoire du Royaume au motif que leurs constatations sont dénuées de toute valeur probante. Elle refuse d'examiner si, en l'espèce, l'illégalité prêtée à l'intervention de la police française compromet le droit à un procès équitable ou entache la fiabilité de la preuve. Il s'ensuit que la Cour de cassation accueille le moyen fondé sur le défaut de justification de leur décision par les juges d'appel et casse, en conséquence, l'arrêt entrepris.

La seconde chambre de la Cour de cassation rappelle les deux critères dont le magistrat peut retenir dans son appréciation du caractère admissible et en ajoute trois, à savoir, d'une part, le caractère purement formel de l'irrégularité, la circonstance que l'illégalité n'est pas intentionnelle, d'autre part, et, enfin, la circonstance que la preuve obtenue illicitement ne concerne qu'un élément matériel de l'infraction.

47. Nonobstant les termes généraux utilisés par la Cour de cassation, les arrêts qui précèdent ont été prononcés en matière pénale. La question consiste à savoir si cette jurisprudence peut être appliquée dans les litiges civils. Certains ont répondu par l'affirmative à la lecture de l'arrêt du 10 mars 2008⁵⁷ de la Cour de cassation rendue en matière civile.

Les faits qui ont donné lieu à cet arrêt peuvent être résumés comme suit : la police entend une personne – bénéficiaire d'allocations de chômage – qui déclare aider régulièrement son frère dans la tenue de son commerce. Procès-

verbal de cette audition est non seulement dressé, mais de surcroît communiqué à l'ONEM. À la suite de cette communication, l'ONEM prend la décision d'enquêter sur la situation du chômeur et, à l'issue de son enquête, de l'exclure du bénéfice des allocations de chômage.

La cour du travail d'Anvers a, aux termes de son arrêt du 26 avril 2007, annulé la décision administrative de l'ONEM, au motif qu'elle se justifie par le seul procès-verbal de la police dont la communication à l'ONEM est irrégulière. La Cour du travail d'Anvers a refusé de faire application de la jurisprudence *Antigone* dès lors que la contestation dont elle a à connaître est de nature civile et que la jurisprudence *Antigone* a été rendue dans des procédures pénales dont les règles en matière de preuve seraient totalement différentes.

L'ONEM se pourvoit en cassation et fait grief aux juges d'appel de ne pas avoir légalement justifié leur décision en refusant d'apprécier le caractère admissible de la preuve illicite. La Cour de cassation, en sa troisième chambre, considère le moyen fondé et casse l'arrêt attaqué. Elle rappelle, en des termes similaires aux arrêts précités, que :

« le juge qui procède à cette appréciation peut notamment tenir compte d'une ou de plusieurs des circonstances suivantes : le caractère purement formel de l'irrégularité, sa conséquence sur le droit ou la liberté protégés par la règle violée, la circonstance que l'autorité compétente pour la recherche, l'instruction et la poursuite des infractions a commis ou n'a pas commis l'irrégularité intentionnellement, la circonstance que la gravité de l'infraction excède manifestement celle de l'irrégularité, le fait que la preuve illicitement recueillie porte uniquement sur un élément matériel de l'infraction, le fait que l'irrégularité qui a précédé ou contribué à établir l'infraction est hors de proportion avec la gravité de l'infraction ».

2) L'arrêt Lee Davies de la Cour européenne des droits de l'homme

48. La jurisprudence *Antigone* a été validée par la Cour européenne des droits de l'homme aux termes de l'affaire *Davies c. Belgique* du 28 juillet 2009⁵⁸. Dans cette affaire, le requérant faisait grief à la Cour de cassation, aux termes d'un arrêt du 16 novembre 2004, d'avoir violé de l'article 6, § 1^{er}, de la CEDH, en raison du fait que les éléments de preuve ayant servi de base aux poursuites

⁵⁶ Cass., 12 octobre 2005, n° P050119F, www.cass.be, lien direct : http://jre.juridat.just.fgov.be/pdfapp/download_blob?ldpdf=F-20051012-16.

⁵⁷ Cass., 10 mars 2008, n° S.07.0073.N, www.cass.be, lien direct : http://jre.juridat.just.fgov.be/pdfapp/download_blob?ldpdf=F-20080310-8.

⁵⁸ Cour eur. D.H., *Lee Davies c. Belgique*, 28 juillet 2009, *Public*, Cour eur. D.H., deuxième section, n° 18704/05, lien direct : <http://hudoc.echrcoe.int/sites/fra/pages/search.aspx?i=001-93820>.

engagées contre lui avaient été recueillies de manière irrégulière⁵⁹. En somme était posée la question de la compatibilité de la jurisprudence récente de la Cour de cassation avec la garantie du droit à un procès équitable.

En l'espèce, la Cour de Strasbourg répondra par l'affirmative dans la mesure où les éléments de preuve litigieux recueillis ne font aucunement douter de leur fiabilité ou de leur exactitude et où le requérant s'est vu offrir la possibilité de contester devant trois degrés de juridiction les éléments recueillis et les constatations faites et de s'opposer à leur utilisation. Elle conclut, en conséquence, en l'absence de violation de l'article 6, § 1^{er}, de la CEDH⁶⁰.

3) *L'arrêt du 5 juillet 2011 du Tribunal de la fonction publique de l'Union européenne*

49. Il est intéressant de comparer la jurisprudence de notre Cour de cassation à celle du Tribunal de la fonction publique de l'Union européenne, et plus particulièrement à celle illustrée par l'arrêt du 5 juillet 2011⁶¹ en matière de protection de la vie privée dans un contexte à la fois professionnel, mais aussi médical. À l'occasion de cet arrêt, le Tribunal s'interroge sur le caractère licite de la prise de connaissance par le Parlement du dossier médical d'une candidate à un emploi d'agent contractuel, initialement constitué et détenu par la Commission. Il examine, ensuite, la validité de la décision prise par le Parlement sur la base de cet ancien dossier médical. Dans le cadre du règlement 45/2001, le Tribunal de la fonction publique conclut, en l'espèce, au caractère illicite du transfert de dossier médical entre institutions européennes et de la décision qui en a résulté. Ce faisant, le Tribunal fait application du principe de l'exclusion de la preuve irrégulière ou illégale⁶².

⁵⁹ La motivation de l'arrêt du 16 novembre 2004 est similaire à celle des arrêts cités *supra* : « Attendu qu'il ne résulte ni de l'article 6 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, qui garantit un procès équitable, ni de l'article 8 de cette Convention, qui consacre le droit au respect de la vie privée et familiale, du domicile et de la correspondance, ni d'aucune disposition constitutionnelle ou légale que la preuve qui a été obtenue en méconnaissance d'un droit fondamental garanti par la Convention précitée ou par la Constitution n'est jamais admissible; attendu que, sauf dans le cas où une disposition conventionnelle ou légale prévoit elle-même les conséquences juridiques de la méconnaissance d'une formalité prescrite par la loi relative à l'obtention de la preuve, le juge décide quelles sont les conséquences de cette irrégularité; que la circonstance que la formalité dont la méconnaissance est constatée concerne un des droits fondamentaux garantis par les articles 6 et 8.1 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales et par les articles 12, alinéa 2, et 15 de la Constitution n'y déroge pas ».

⁶⁰ Cour eur. D.H., *Lee Davies c. Belgique*, 28 juillet 2009, *op. cit.*, §§ 53 et 54.

⁶¹ Cette décision a été examinée et fait l'objet d'une note d'observations. F. OMRANI et J.-M. VAN GYSEGHEM, « Quand le transfert des données "santé" est illégal », note sous Tribunal de la fonction publique de l'Union européenne (1^{re} ch.), 7 juillet 2011, *R.D.T.J.*, n° 45, Bruxelles, Larcier, pp. 121-149.

⁶² Voy. en particulier les §§ 137 et s.

4) *L'application de la jurisprudence par les juridictions du travail*

50. Après quelques hésitations, les Cours du travail de Mons⁶³, Liège⁶⁴ et Anvers⁶⁵ ont considéré que l'enseignement de la Cour de cassation quant à l'admissibilité de preuves recueillies de manière illicite était applicable dans le cadre d'un litige relatif à la rupture des relations contractuelles entre un travailleur et son employeur.

51. La Cour du travail de Bruxelles, quant à elle, considère que la Cour de cassation n'a certainement pas voulu qu'un employeur puisse impunément porter atteinte à des droits et à des libertés aussi fondamentaux. Déjà dans un arrêt du 15 juin 2006⁶⁶, elle avait refusé d'appliquer la jurisprudence résultant de l'arrêt *Manon* au motif qu'il était prononcé en matière pénale et que la comparaison qu'il effectue entre la gravité de l'infraction commise lors du recueillement de la preuve et/ou de l'information litigieuse et la gravité de l'infraction illicite constatée ne serait pas pertinente en droit civil où le débat ne porte nullement sur la constatation ou non d'une infraction. À l'occasion d'un récent arrêt du 7 février 2013⁶⁷, l'arrêt *RTL*, la Cour du travail de Bruxelles confirme sa jurisprudence antérieure et fait fi de l'arrêt précité du 10 mars 2008. Elle considère que les critères énoncés par la Cour de cassation dans son arrêt sont conçus pour le droit pénal ou les litiges ayant une nature pénale et que la Cour de cassation n'a certainement pas voulu qu'un employeur puisse impunément porter atteinte à des droits et à des libertés fondamentaux à seule fin de pouvoir établir un motif grave qu'aurait commis un travailleur et qui n'est même pas constitutif d'une infraction pénale.

52. Les considérations retenues par la Cour du travail de Bruxelles nous paraissent contestables. En effet, il peut être fait remarquer que si les règles pénales diffèrent des règles civiles, c'est dans le sens d'une plus grande exigence notamment au regard du droit à un procès équitable. Ainsi peut-on considérer que si la preuve est admise en matière pénale, il devrait en être d'autant plus ainsi en matière civile.

À cela s'ajoute qu'il est inexact d'affirmer que l'admissibilité de la preuve illicite aboutit à l'impunité des violations du droit au respect de la vie privée. En effet, rien ne s'oppose à ce que le parquet, d'initiative ou à la suite de la plainte ou de la constitution de partie civile par la personne protégée, poursuive l'employeur

⁶³ C. trav. Mons, 8 décembre 2010, *Chron. D.S.*, 2011, p. 399.

⁶⁴ C. trav. Liège, 8 mars 2011, *Chron. D.S.*, 2011, p. 404.

⁶⁵ C. trav. Anvers (sect. Hasselt), 2 septembre 2008, *Orientations*, 2009, p. 22, note K. ROSIER.

⁶⁶ C. trav. Bruxelles, 15 juin 2006, *R.G.* n° 48484, <http://jre.juridat.just.fgov.be/>, lien direct : http://jre.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20060615-5.

⁶⁷ C. trav. Bruxelles (2^e ch.), 7 février 2013, n° 2012/AB/1115, <http://jre.juridat.just.fgov.be/>, lien direct : http://jre.juridat.just.fgov.be/pdfapp/download_blob?idpdf=F-20130207-2.

pour violation du droit à la vie privée du travailleur. De même, rien n'interdit au travailleur d'introduire une demande tendant au paiement d'une indemnité résultant de la violation de son droit au respect de la vie privée.

À nos yeux, *de lege lata*, une décision juste consisterait tout à la fois à permettre à l'employeur de faire usage de la preuve illicite conformément à la jurisprudence dite *Antigone*, mais aussi à reconnaître la violation du droit au respect de la vie privée et, le cas échéant, accorder à ce titre une indemnité au travailleur – sans préjudice de la sanction pénale.

D. Conclusion quant au régime légal

53. L'objectif poursuivi par cette première section est double. D'une part, il s'agissait de familiariser le lecteur avec les principales règles légales qui trouvent à s'appliquer. Il s'agissait ensuite de montrer la difficulté de les appliquer dans le contexte particulier du travail. Cette inapplicabilité et inadéquation ont contraint le Conseil national du travail à adopter des règles destinées à assouplir le système en place par le biais de conventions collectives du travail rendues obligatoires par arrêtés royaux. Toutefois, toutes les dispositions des CCT n° 68, n° 81 et n° 89 qui dérogent à la loi vie privée, à la loi relative aux communications électroniques et à l'article 314bis du Code pénal sont tout à la fois illégales, nulles et même inconstitutionnelles en sorte que ces dérogations sont, en définitive, sans effet.

Comme si le cadre juridique n'était pas déjà assez complexe, il faut en outre tenir compte de l'adoption dans les prochains mois d'un règlement européen – par nature directement applicable – appelé à remplacer la directive 95/46.

54. La seule échappatoire pratique et légale résulte de la jurisprudence dite *Antigone* puisqu'elle permet à l'employeur – dans certaines conditions – de se prévaloir des conséquences tirées d'un élément de preuve obtenu de manière illicite. Cette jurisprudence n'est, toutefois, pas (encore) unanimement admise par les commentateurs ou par les juridictions du travail. Ainsi, la Cour du travail de Bruxelles reste-t-elle sourde à la jurisprudence de la Cour de cassation et maintient-elle sa jurisprudence antérieure en dépit de l'arrêt du 8 mars 2008.

55. Le droit positif ne rencontre pas l'impératif de sécurité juridique. En effet, il n'est pas possible aujourd'hui d'affirmer qu'un contrôle de l'employeur qui répondrait aux exigences des CCT n° 68, n° 81 ou n° 89 est légal. Aucune assurance non plus quant à la possibilité d'utiliser le résultat de ce contrôle dans le cadre d'une procédure qui permettrait de rompre le contrat de travail. Le système actuel est le résultat de bricolages qui sont le fruit des efforts des partenaires sociaux, de l'autorité de contrôle et de la jurisprudence. Ces bricolages font parfois l'effet d'un emplâtre sur une jambe de bois. La seule réelle solution

consiste à appeler de ses vœux l'adoption d'un régime dérogatoire spécifique à la vie privée dans le cadre du travail.

56. C'est à la lumière de ces considérations qu'il faudra apprécier les développements des deux prochaines sections dédiées, d'une part, à la question de la validité du consentement du travailleur (section 2, § 1^{er}) et à l'examen de certains outils de communication (section 2, § 2), d'autre part.

Section 2

Le consentement du travailleur et certains outils de communication

§ 1. Le consentement du travailleur

A. Le consentement – une cause de légitimation précaire du traitement de données

57. Comme résumé *supra* au paragraphe 8, le traitement des données à caractère personnel pour être valable doit non seulement répondre des conditions de fond, mais également intervenir dans une des hypothèses de légitimation de l'article 5 de la loi vie privée. En particulier, on s'intéresse à présent à l'hypothèse où la personne concernée a indubitablement donné son consentement.

L'article 1^{er}, § 8, de la loi vie privée énonce que le consentement de la personne concernée résulte de toute manifestation de volonté, libre, spécifique et informée par laquelle elle accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.

Ce consentement doit être préalable, mais n'est soumis à aucune forme particulière – si ce n'est que le responsable du traitement avisé veillera naturellement à se constituer une preuve de ce que la personne concernée a effectivement consenti au traitement de ses données.

58. À côté du régime général, il existe un régime d'exception pour les données dites sensibles. Rappelons brièvement que les données sensibles sont les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ou qui ont trait à la vie sexuelle de la personne concernée, qui ont trait à sa santé, ou encore constituent des données judiciaires. Ces données, par leur nature, justifient la mise en place d'une protection accrue⁶⁸. Dans le cadre du consentement, celle-ci se manifeste par l'exigence d'un consentement sous la forme écrite qui, de surcroît, peut être retiré à tout moment.

Remarquons que le caractère sensible d'une donnée n'est pas toujours prévisible ou apparent pour l'employeur. À titre d'exemple, citons les données rela-

⁶⁸ Voy. les articles 6 et suivants de la loi vie privée.

tives à la santé dont l'acceptation est large puisque toutes données qui informent sur l'état de santé ou de maladie, tant d'un point de vue physique que psychique, d'une personne identifiée ou identifiable entre dans cette catégorie. Sont donc visées les informations relatives à une pathologie grave (cancer du pancréas) ou perçue comme honteuse (SIDA), mais aussi les informations plus anodines comme celles relatives à un pied blessé⁶⁹. On imagine aisément que les travailleurs auront la volonté de prendre des précautions particulières lorsqu'il sera question de mentionner des problèmes liés à une maladie génétique ou dégénérative. Dans ce cas, ils veilleront probablement à ne pas utiliser l'adresse professionnelle de courriel mise à leur disposition ou à indiquer clairement qu'il s'agit d'un courriel personnel. La réponse à la question de savoir si les travailleurs feront preuve du même soin à l'égard de courriels faisant état, à la marge, de maux d'hiver (rhume, grippe, etc.) ou encore des allergies de printemps est plus incertaine et se traduit, dans le chef de l'employeur, par la nécessité de l'obtention d'un consentement écrit.

59. La légitimation fondée sur le consentement semble *a priori* constituer une voie facile. *A priori* seulement dès lors qu'au-delà des difficultés d'obtenir un consentement valable, encore faut-il garder à l'esprit que ce consentement peut être retiré à tout moment. Ceci n'est pas sans poser de difficultés lorsque le traitement n'est légitimé que par le seul consentement de la personne concernée.

La difficulté est limitée lorsque la relation qui existe entre le responsable de traitement et la personne concernée est ponctuelle parce qu'elle s'inscrit, par exemple, dans le cadre de contrats à prestations uniques. On songe notamment aux contrats de vente où le responsable du traitement n'est amené à traiter qu'une seule fois des données de la personne concernée. Ainsi, si la personne concernée venait à changer d'avis, l'absence de consentement ou plutôt la survenance d'un défaut de consentement ne vaudrait que pour le futur et, partant, ne ferait obstacle qu'au seul traitement ultérieur des données à caractère personnel (par opposition au traitement primaire). On sent tout de suite dans ce cas qu'il doit exister une autre cause de légitimation du traitement de données à caractère personnel, à savoir l'exécution du contrat sollicité par la personne concernée elle-même.

Dans un contrat à prestations successives, comme l'est le contrat de travail, le retrait par la personne concernée de son consentement pourrait faire obstacle non seulement au traitement ultérieur, mais aussi à la poursuite du traitement primaire. L'usage du conditionnel est volontaire et résulte de ce qu'il faut également envisager que le retrait du consentement de la personne concernée puisse, dans certains cas, être considéré comme abusif, en sorte qu'en ramenant

⁶⁹ C.J.C.E., 6 novembre 2003, *Lindqvist c. Suède*, Rec. C.J.C.E., 2003, p. I-13014, C-101/01, §§ 49 à 51.

le droit à son usage normal, cela pourrait autoriser le responsable du traitement de poursuivre pendant un certain temps son traitement.

B. Le consentement – une condition dérogatoire au régime d'interdiction

60. Le consentement est donc une cause de légitimation du traitement de données à caractère personnel qui est précaire. Si on s'y intéresse néanmoins, c'est précisément parce qu'il est au centre de la faculté de surveillance et de contrôle de l'employeur opéré par le biais des communications électroniques. En effet, rappelons que l'article 124 de la loi relative aux communications électroniques interdit tout traitement opéré par un tiers à une communication électronique sur cette communication s'il n'y a pas été autorisé par toutes les personnes concernées directement ou indirectement⁷⁰. Le consentement est donc obligatoire non pas au regard de la loi vie privée et de son exigence de légitimation, mais bien dans le cadre du régime spécifique de la communication électronique et de sa prise de connaissance par un tiers. C'est ce même consentement qui est visé par l'article 314bis du Code pénal. Dans ce cadre, le consentement de la personne concernée n'est plus une cause, parmi d'autres, de légitimation du traitement, mais bien une condition de celui-ci.

61. Il est acquis, dans notre ordre juridique interne, que le principe est l'autonomie de la volonté. Les parties sont libres de conclure tout contrat avec pour seule limite leur imagination et le respect de l'ordre public⁷¹, des bonnes mœurs⁷², et des lois impératives conformément aux articles 6 et 1134 du Code civil. On enseigne que si l'ordre public protège l'intérêt général, les dispositions impératives protègent – quant à elles – des intérêts privés. Ceci implique un régime différencié quant à la sanction de la méconnaissance et qui sera, selon les cas, soit la nullité absolue soit la nullité relative. Le régime différencié s'exprime également à l'égard de la possibilité de déroger contractuellement à ces règles. Toutefois, dans le cadre du consentement du travailleur au traitement des données qui le concernent, il nous paraît inexact de l'examiner sous l'angle de la renonciation à un droit fondamental alors qu'il s'agit de la mise en œuvre d'une condition objective au sein d'un régime dérogatoire. La personne protégée s'abstient en d'autres termes de mettre en œuvre un droit, à savoir le droit de s'opposer au traitement de données qui la concerne. Elle ne renonce

⁷⁰ Voy. *supra*, §§ 14 et s.

⁷¹ Selon une jurisprudence constante, « n'est d'ordre public que la loi qui touche aux intérêts essentiels de l'État ou de la collectivité ou qui fixe, dans le droit privé, les bases juridiques sur lesquelles repose l'ordre économique ou moral de la société ». Voy. notamment Cass, 9 décembre 1948, *Pas.*, I, p. 699; Cass., 15 mars 1968, *Pas.*, I, p. 894; Cass., 10 novembre 1978, *Pas.*, 1979, I, p. 309; Cass., 28 septembre 1979, *Pas.*, 1980, I, p. 131.

⁷² De même, la notion de bonnes mœurs correspond-elle « à une morale coutumière faite d'habitudes et de traditions d'un peuple et est en évolution constante avec l'état d'esprit d'une civilisation ». Voy. notamment Liège, 22 novembre 1979, *Jur. Lg.*, 1980, p. 1.

nullement au droit à la vie privée qui reste inaliénable. C'est tellement vrai que le consentement de la personne protégée ne peut porter sur les conditions dans lesquelles le traitement interviendrait. Ainsi ne serait-il pas possible pour la personne concernée de consentir à un traitement qui ne serait ni loyal ni licite ou encore qui porterait sur des données excessives ou non pertinentes au regard de la finalité du traitement.

C. Le consentement libre du travailleur

62. Une autre difficulté résulte du rapport hiérarchique qui existe entre le travailleur et l'employeur. Un consentement libre est-il possible dans ce contexte ? La C.P.V.P. répond par la négative aux termes de la recommandation 08/2012 puisqu'elle exclut la possibilité même pour le travailleur d'émettre un consentement libre⁷³. Ainsi, selon la C.P.V.P. la relation de travail ne permet pas de garantir le caractère libre du consentement compte tenu du déséquilibre de la relation contractuelle.

63. Le point de vue de la C.P.V.P. est contestable⁷⁴, et ce, pour plusieurs raisons. La première est « qu'il ne ressort d'aucune disposition légale que le consentement donné à une convention par une partie économiquement faible est toujours dénué de validité » ou serait nécessairement « obtenu à la suite d'erreur, de violence ou de dol et que, par conséquent, il n'était pas valable »⁷⁵. En pratique, du reste, les juridictions du travail tiennent compte du consentement du travailleur au traitement des données à caractère personnel qui le concernent pour apprécier le caractère licite d'une preuve qui est produite par l'employeur. Cette prise en considération implique nécessairement que les magistrats du travail n'excluent pas, *a priori*, la validité du consentement du travailleur⁷⁶. La Cour du travail d'Anvers va même plus loin puisqu'elle retient même un consentement implicite : la communication à un collègue par la travailleuse de son mot de passe donnant accès à son courrier électronique emporte son consentement à ce que ce collègue consulte ledit courrier électronique⁷⁷.

64. À cela s'ajoute qu'il faut considérer que le régime organisé par l'article 27 de l'arrêté royal du 13 février 2001 portant exécution de la loi vie privée est un régime dérogatoire au droit commun en interdisant, dans le cadre du traitement de données sensibles visées aux articles 6 et 7 de la loi vie privée, un traitement qui serait justifié par le seul consentement du travailleur. Il est uniquement fait exception à cette interdiction lorsque le traitement vise l'octroi d'un avantage à la personne concernée.

65. Enfin, il serait illogique d'affirmer que le travailleur consent valablement au contrat de travail et notamment à l'égard de la nature des prestations à fournir, du montant de sa rémunération et des différents avantages dont il bénéficie, du lieu de la réalisation du travail, du code vestimentaire, etc., mais ne pourrait pas valablement consentir au traitement des données à caractère personnel qui le concernent.

66. En réalité, il ne peut être affirmé que le consentement qui porte sur un tel traitement *a priori* rencontre ou méconnaît les exigences de la loi. Il nous paraît que la disparité des circonstances doit amener à des solutions contrastées. Ainsi, la validité du consentement du travailleur devra-t-elle être examinée différemment selon que le travailleur est un employé « ordinaire », un cadre supérieur, un ouvrier ou un travailleur indépendant.

D. Le moment où le consentement du travailleur est donné

67. Toute personne bénéficie du droit au respect de sa vie privée. Ce droit, lié à la personnalité, est inhérent à toute personne vivante. Dans la mesure où le droit à la vie privée préexiste à la relation contractuelle se pose naturellement la question du moment où le consentement du travailleur au traitement des données à caractère personnel qui le concernent doit être formulé.

Il n'est pas contesté que le consentement du travailleur doit être antérieur au traitement des données qui le concernent. La question qui nous occupe est de savoir si le consentement au traitement de données à caractère personnel doit intervenir avant, pendant ou après le consentement à la relation contractuelle qui est la raison d'être du traitement précité. En réalité, cela revient à se poser la question de savoir si le lien contractuel a une incidence effective sur le consentement du travailleur au traitement des données qui le concernent. Le postulat de la réflexion est que le consentement du travailleur ne serait ni sincère ni libre dans la mesure où son refus ferait obstacle à la conclusion du contrat de travail ou à la poursuite de la relation de travail. Cette thèse doit être nuancée.

68. Lorsqu'il est donné préalablement à la conclusion du contrat de travail, il ne peut être contesté que le consentement du travailleur peut résulter d'un choix en opportunité et en connaissance de cause dans le chef du travailleur compte

⁷³ Voy. §§ 53 et s. de la recommandation 08/2012.

⁷⁴ Voy. en ce sens S. GILSON, F. LAMBINET, K. ROSIER, *Le droit au respect de la vie privée du travailleur. État des lieux*, Limal, Anthemis, CRIDS, 2012, p. 17, n° 12 « En effet, dans l'analyse civiliste classique, le fait que le travailleur se trouve dans une position économiquement plus faible ne suffit pas à considérer que son accord est vicié de ce fait, sauf à démontrer l'abus d'une position dominante » et jurisprudence citée.

⁷⁵ Cass., 2 mai 1969, Pas., 1969, I, p. 781.

⁷⁶ Voy. notamment Trib. trav. Bruxelles, 4 décembre 2007, J.T.T., 2008, n° 1005, 179. Voy. également à ce sujet C. trav. Bruxelles, 3 mai 2006, J.T.T., 2006, p. 262 ; C. trav. Bruxelles, 13 septembre 2005, *Computerr.*, 2006, p. 100 ; C. trav. Anvers (sect. d'Anvers), 15 décembre 2004, *Chr. D. S.*, 2006, p. 146 ; C. trav. Bruxelles (3^e ch.), 10 février 2004, *Orientatie*, 2004, p. 3 ; C. trav. Anvers (sect. Anvers), 1^{er} octobre 2003, J.T.T., 2004, p. 510 ; Trib. trav. Hasselt (1^{re} ch.), 21 octobre 2002, *Chron. D. S.*, 2004, p. 197.

⁷⁷ C. trav. Anvers (sect. Anvers), 8 janvier 2003, *Chr. D. S.*, 2003, p. 193 ; R.W., 2005-2006, p. 391.

tenu des garde-fous légaux. Rien ne justifie la considération selon laquelle, en toute hypothèse, cette décision particulière ne serait pas prise librement alors qu'il n'est pas contesté que d'autres choix tout aussi importants aux yeux du travailleur⁷⁸ puissent l'être. Il en est d'autant plus ainsi que le consentement du travailleur ne peut justifier ni une méconnaissance des dispositions pénales⁷⁹ ni une méconnaissance des exigences énoncées à l'article 4 de la loi vie privée en termes de finalité, proportionnalité, légitimité et de légalité⁸⁰.

69. Lorsque le consentement au traitement des données à caractère personnel intervient après la conclusion du contrat de travail, il nous paraît plus libre encore dans la mesure où il peut être considéré que le travailleur est débarrassé de la pression résultant de la crainte de ne pas se faire offrir le travail en question. Certes, dans le cadre d'un contrat à durée déterminée, on peut concevoir théoriquement qu'un refus du travailleur puisse faire obstacle au renouvellement de ce contrat. Cependant, ce caractère précaire est inhérent au contrat de travail à durée déterminée ce qui explique que le régime soit réglementé et qu'une conversion en contrat à durée indéterminée soit organisée par la loi.

Dans le cadre d'un contrat à durée indéterminée, peut-on sérieusement imaginer qu'un employeur ait envie de se séparer d'un travailleur pour le seul motif d'un refus de consentir au traitement des données qui le concernent? Rappelons, à cet égard, qu'en droit belge le licenciement des travailleurs est une matière réglementée strictement. Ainsi, s'agissant des ouvriers, la loi présume que leur licenciement est abusif. Il appartient à l'employeur d'apporter la preuve inverse. Cette preuve ne peut porter que sur la justification du licenciement abusif et, à ce titre, seuls deux motifs sont admis, à savoir, d'une part, des motifs économiques et, d'autre part, des motifs liés au comportement de l'ouvrier. À défaut d'apporter une telle preuve, l'employeur est redevable d'une indemnité équivalant à six mois de rémunérations brutes, sans préjudice des frais et dépens, en ce compris l'indemnité de procédure. À l'égard des employés, leur licenciement est soumis à un préavis ou à une indemnité compensatoire de préavis qui est fonction de leur ancienneté. L'employeur n'est pas à l'abri d'une procédure que mettrait en œuvre l'employé du chef de licenciement abusif. Si le grief devait être fondé – ce qui serait nécessairement le cas dans notre hypothèse⁸¹ –, il sera en outre redevable du paiement d'une indemnité pour licenciement abusif qui peut excéder six mois de rémunérations brutes.

⁷⁸ Voy. notamment les choix mentionnés *supra* au § 65.

⁷⁹ Articles 314bis du Code pénal et 124 et 125 de la loi relative aux communications électroniques.

⁸⁰ Voy. à cet égard les développements *supra* au § 61.

⁸¹ À savoir, le licenciement d'un employé qui bénéficie d'un contrat de travail à durée indéterminée pour le seul motif qu'il refuse de consentir au traitement des données à caractère personnel qui le concernent.

70. Lorsque le consentement est donné concomitamment à la conclusion du contrat, il réunit les circonstances visées aux paragraphes 68 et 69 auxquels il est renvoyé. Pour le surplus, il faudra être vigilant au respect de la condition de spécificité du consentement. À cet égard, la prudence recommande, dans cette hypothèse, de rédiger *a minima* une clause distincte au sein du contrat de travail.

E. Conclusion quant au consentement

71. Le consentement du travailleur peut donc être soit une cause de légitimation du traitement visée à l'article 5 de la loi vie privée, soit une condition du régime dérogatoire aux articles 124 de la loi relative aux communications électroniques et 314bis du Code pénal, soit les deux à la fois.

Il nous paraît que la C.R.V.P. a trop rapidement écarté l'hypothèse que le travailleur puisse valablement consentir au traitement des données à caractère personnel qui le concernent par son employeur puisque la portée du consentement est limitée en ce qu'elle ne permet pas de déroger aux règles impératives de la loi de la vie privée, de la loi relative aux communications électroniques ni aux dispositions pénales.

À n'en pas douter, la législation en matière de licenciement des travailleurs renforce la protection en dissuadant l'employeur peu scrupuleux de mettre légèrement un terme au contrat de travail.

Aussi, si le traitement de données à caractère personnel est à ce point essentiel pour l'entreprise que l'employeur est prêt à prendre le risque de se voir opposer un licenciement abusif, il est fort probable que le traitement se justifie par une autre hypothèse de l'article 5 de la vie privée, parce qu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci, au respect d'une obligation à laquelle l'employeur est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance, à la sauvegarde de l'intérêt vital de la personne concernée, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées, ou encore 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.

§ 2. Applications pratiques

A. Rappel des exigences en matière de traitement de données à caractère personnel

72. L'ensemble des règles énumérées *supra* à la première section peut être résumé dans le tableau schématique :

Régime général du traitement de données à caractère personnel	
La finalité	✓ Déterminée, explicite et légitime ✓ Pas de traitement ultérieur incompatible
La proportionnalité	✓ Les données sont adéquates, pertinentes et non excessives au regard de la finalité ✓ Les données sont exactes et, si nécessaire, mises à jour ✓ Le choix de la voie la moins attentatoire
La légalité	✓ Traitement loyal et licite des données
La durée limitée de conservation	✓ Conservation sous une forme permettant l'identification pendant une durée n'excédant pas celle nécessaire à la réalisation de la finalité
La sécurité et la confidentialité	✓ Mise en place d'un système qui offre des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives au traitement ✓ Limiter les accès en fonction des nécessités de service ✓ Prendre les mesures techniques et organisationnelles requises pour protéger les données à caractère personnel contre la destruction accidentelle ou non autorisée, contre la perte accidentelle ainsi que contre la modification, l'accès et tout autre traitement non autorisé
La transparence	✓ Déclaration préalable auprès de la C.P.V.P. ✓ Information à fournir à la personne concernée portant sur - o l'identité du responsable du traitement; - o les finalités poursuivies; - o les destinataires ou les catégories de destinataires des données; - o le caractère obligatoire ou non de la réponse ainsi que les conséquences éventuelles d'un défaut de réponse; - o l'existence d'un droit d'accès et de rectification des données; - o les données faisant l'objet du traitement; - o les recours que la personne protégée peut exercer. ✓ Concertation et publicité de la politique de contrôle de l'employeur

La cause de légitimation	✓ Caractère indubitable du consentement de la personne concernée (voy. <i>infra</i>) ou ✓ Nécessité d'exécuter un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ou ✓ Nécessité de respecter une obligation, à laquelle l'employeur est soumis par ou en vertu d'une loi, d'un décret ou d'une ordonnance, à la sauvegarde de l'intérêt vital de la personne concernée ou ✓ Nécessité d'exécuter une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ou ✓ Nécessité de réaliser 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
Le consentement	✓ Libre, spécifique, informé, préalable et indubitable ✓ Écrit pour les données sensibles ✓ Ne constitue pas une cause de justification lorsqu'il porte sur des données relatives à la santé et qu'il est donné par un travailleur à son employeur
Les données sensibles	✓ Existence d'un régime dérogatoire
Les droits de la personne protégée	✓ Le droit d'accès aux données personnelles ✓ Le droit de rectification d'une donnée inexacte ✓ Le droit de solliciter des informations au sujet du traitement ✓ Le droit de s'opposer au traitement des données personnelles qui la concernent
Le contrôle de l'employeur / L'accès à certaines données	✓ Ponctuel ✓ Justifié - o par une utilisation abusive des outils de travail, - o par un comportement contraire à l'ordre public ou aux bonnes mœurs de l'employé, - o par une obligation légale, par l'intérêt légitime de l'employeur de contrôler la qualité du travail, le temps du travail, - o par la sécurité du réseau. ✓ Poursuite de l'activité suite à l'absence du travailleur pour maladie, par suite de la fin du contrat de travail, suite au décès du travailleur

B. La correspondance

73. La correspondance écrite reste le moyen de communication par excellence dans le cadre de la relation de travail. Cette correspondance est aujourd'hui principalement électronique bien que la correspondance ordinaire (non dématérialisée) soit toujours utilisée.

1) Les correspondances ordinaires

74. Les lettres bénéficient d'une protection particulière conférée par l'article 29 de la constitution qui dispose que « le secret des lettres est inviolable ». Toutefois, il est admis qu'une lettre adressée à l'employé d'une entreprise n'implique pas que cet employé en soit le destinataire réel, mais uniquement le destinataire fonctionnel. Personne ne conteste que ce soit bien la société qui est destinataire de la missive et qu'il peut être considéré, *a priori*, que tout courrier adressé au siège de l'entreprise est un courrier adressé à l'entreprise elle-même. Il n'en est autrement que dans la mesure où des mentions spécifiques contraires sont apposées sur la correspondance envisagée⁸².

2) Les courriels sont-ils des lettres ? Sont-ils des correspondances ?

75. Les courriels ne bénéficient en principe pas de la protection constitutionnelle de l'article 29 dans la mesure où ils ne répondent pas à la définition de lettre confiée à un service postal⁸³.

76. Si les courriels ne sont pas des lettres au sens de l'article 29 de la Constitution, constituent-ils une correspondance protégée par l'article 8 de la CEDH ? À cette question, il faut répondre par l'affirmative même lorsque ces correspondances revêtent un caractère professionnel.

À l'occasion de l'arrêt *Niemietz*⁸⁴, la Cour européenne des droits de l'homme est amenée à se prononcer quant à la question de savoir si une perquisition dans un local professionnel – en l'occurrence le cabinet d'un avocat – constitue, ou non, une violation de la vie privée d'un individu et, plus particulièrement, une violation de son droit au respect de son domicile et de sa correspondance. La demande est introduite par M. Niemietz qui réside en Allemagne où il exerce la profession d'avocat. Il s'investit, en outre, dans un groupe de travail anticlérical

au sein d'un parti politique local, à savoir la Bunte Liste. M. Niemietz n'est pas adhérent de ce parti, mais travaille activement dans le groupe de travail précité. En décembre 1985, une télécopie est adressée au magistrat cantonal de Freising par le soi-disant Klaus Wegner (peut-être une personne fictive) avec la précision suivante : « au nom du groupe de travail anticlérical de la Bunte Liste de Fribourg » et un numéro de boîte postale. En août 1986, le tribunal cantonal de Munich ordonne une perquisition au cabinet de Me Niemietz en raison d'une enquête préliminaire contre Klaus Wegner pour insultes contrevenant à l'article 185 du Code pénal (allemand) à l'égard du magistrat cantonal de Freising. Le choix du lieu de la perquisition ordonnée résulte de ce que, pendant un certain temps, la distribution du courrier destiné à la Bunte Liste était parfois assurée au cabinet d'avocat de Me Niemietz. Le but poursuivi par cette perquisition est de « découvrir et saisir des documents pouvant révéler l'identité de "Klaus Wegner" ». La perquisition du cabinet de Me Niemietz survient au cours du mois de novembre 1986. Dans cet arrêt de principe, la Cour européenne des droits de l'homme a considéré que des échanges professionnels électroniques constituent bien de la correspondance au sens de l'article 8 de la CEDH et, partant, relèvent de la vie privée.

3) Les courriels envoyés depuis le lieu du travail ou grâce aux outils mis à la disposition du travailleur

77. Le choix de la Cour européenne des droits de l'homme de faire application de l'article 8 de la CEDH dans le cadre de courriels professionnels peut apparaître comme étant essentiellement lié à la qualité d'avocat de M. Niemietz. Cependant, la Cour européenne des droits de l'homme a confirmé et généralisé cet enseignement à l'occasion de l'arrêt *Copland*⁸⁵. Les faits dont la Cour a à connaître peuvent être résumés comme suit : Madame Copland travaille dans un établissement d'enseignement supérieur, le *Carmarthenshire College*, et est l'assistante de son président. Elle travaille également en étroite collaboration avec le vice-président du collège. Du mois d'août 1998 au mois de novembre 1999, à l'instigation du vice-président du collège, furent mis sous surveillance : les appels téléphoniques, le courrier électronique et les connexions internet de la requérante. La surveillance des appels téléphoniques impliquait au minimum une analyse des factures précisant les numéros appelés, les jour, heure, durée et coût des appels. La surveillance du courrier électronique professionnel impliquait, quant à elle, une analyse des adresses électroniques ainsi que des jours et heures d'envoi des messages. Tandis que la surveillance des connexions internet impliquait une analyse des sites consultés, l'heure et la durée de ces visites. Le

⁸² C. trav. Liège, 17 mai 1985, J.T.T., p. 492 ; C. trav. Liège (Namur), 25 avril 2002, *www.cass.be* ; R. ROBERT, « Correspondance et vie privée sur les lieux du travail : une cohabitation difficile », *Orientations*, n° 7, sept. 2008, pp. 18-20.

⁸³ C. trav. Liège, 25 avril 2004, *www.cass.be*. Certains magistrats font cependant explicitement référence à cette disposition constitutionnelle à l'occasion d'un contrôle de la légalité de la prise de connaissance de courriels. Voy. en ce sens Trib. trav. Liège (3^e ch.), 3 septembre 2008, R.G. n° 371.015, *www.cass.be* ; Trib. trav. Liège (3^e ch.), 19 mars 2008, R.G. n° 360.454, *www.cass.be* ; Trib. trav. Verviers (1^{re} ch.), 20 mars 2002, J.T.T., 2002, p. 183.

⁸⁴ Cour eur. D.H., *Niemietz c. Allemagne*, 16 décembre 1992, *Public. Cour eur. D.H.*, série A, n° 251.

⁸⁵ Cour eur. D.H., *Copland c. Royaume-Uni*, 3 avril 2007, *Public. Cour eur. D.H.*, deuxième section, n° 62617/00 ; <http://hudoc.echr.coe.int/>.

but de la surveillance aurait été de vérifier que Madame Copland ne faisait pas un usage excessif des ressources du collège. Selon Madame Copland ses déplacements étaient également surveillés tant dans le cadre professionnel que pendant ses congés annuels ou maladie. Les parties divergent quant à la nature des mesures de surveillance en cause et à leur durée d'application. Cette divergence n'est pas problématique pour la Cour européenne des droits de l'homme, car la question de la violation de l'article 8 de la CEDH se pose même à l'égard des faits reconnus par le gouvernement.

La question soumise à la Cour européenne des droits de l'homme est de déterminer si des messages électroniques envoyés depuis le lieu de travail et les connexions à des sites internet depuis le lieu de travail sont, ou non, compris dans la notion de « vie privée » et de « correspondance ». La Cour européenne des droits de l'homme répond par l'affirmative en retenant une conception large de la notion de vie privée.

78. Dans l'affaire *Copland* précitée, soulignons que les courriels avaient été envoyés grâce aux outils mis à la disposition par le *Carmarthenshire College*. La Cour européenne n'avait déduit aucune considération particulière résultant de cette mise à disposition⁸⁶.

4) L'absence de présomption de caractère professionnel du courriel

79. En France, il est admis que les courriels émis ou reçus grâce à un outil informatique professionnel sont présumés avoir un caractère professionnel, à moins d'être clairement identifiés comme étant « personnels »⁸⁷. À défaut d'une telle identification, l'employeur peut y accéder en dehors de la présence du salarié. Pour ceux qui sont indiqués comme étant « personnels », l'employeur peut en prendre connaissance en présence et avec l'accord du travailleur et, à défaut d'accord, il peut se faire autoriser par un magistrat.

80. En Belgique, ce régime dérogatoire n'a pas cours et il n'existe pas de présomption selon laquelle tout mail adressé à l'adresse professionnelle de l'employé est un courriel professionnel de l'entreprise elle-même.

Tout au contraire, en l'absence de régime dérogatoire spécifique sanctionné par une loi, l'application rigoureuse de la loi vie privée et de la jurisprudence de la Cour européenne ne permet pas de considérer *a priori* que des courriels sont dépourvus de tout caractère personnel. Il n'en va autrement que dans l'hypothèse où les courriels ne sont pas individualisés en recourant à une adresse fonctionnelle collective de type « *secretariat@employeur.be* ».

⁸⁶ *Contra* Trib. trav. Liège (3^e ch.), 19 mars 2008, R.G. n° 360.454, www.cass.be.

⁸⁷ Cass. fr., 16 janvier 1992, www.legifrance.gouv.fr ; Cass. fr., 3 octobre 2006, *Comm. Electronique*, mars 2007, n°3, p. 47.

81. La prudence recommande à l'employeur d'adopter une charte qui porte notamment sur l'utilisation des courriers électroniques. Cette charte énoncerait les règles relatives à l'utilisation de l'adresse professionnelle de courriel, à l'utilisation occasionnelle et limitée d'une adresse personnelle – le cas échéant, en interdisant l'usage privé de l'adresse professionnelle. On pense notamment à un engagement de l'employé, d'une part, d'utiliser l'adresse de courriel exclusivement aux fins d'exécuter les tâches qui lui sont confiées et, d'autre part, dans le cadre de messages privés, de s'abstenir d'y inclure un élément susceptible de le relier à l'entreprise que ce soit par l'usage d'une signature professionnelle, d'un titre professionnel ou de toute autre mention susceptible de favoriser chez le destinataire l'impression que le message a été écrit par l'entreprise ou envoyé sous sa supervision et approbation. Il peut, de surcroît, être interdit à l'employé de faire usage d'une adresse courriel privée pour avoir un échange épistolaire professionnel. Enfin, on songera à prévoir le comportement à adopter par l'employé s'il reçoit un courriel professionnel dans sa messagerie privée ou s'il reçoit un courriel privé dans sa messagerie professionnelle.

5) Le contrôle des courriels par l'employeur

82. Il est bon de rappeler ici la position de la C.P.V.P. au sujet du contrôle opéré à l'égard des correspondances électroniques dès lors qu'elle ne laisse place à aucune interprétation. Elle affirme en effet que « la prise de connaissance du contenu des courriers électroniques est excessive et contraire aux dispositions légales mentionnées *supra*, de la même façon que le seraient l'écoute et/ou l'enregistrement des communications téléphoniques de l'employé »⁸⁸. Ceci doit indubitablement inciter à la plus grande circonspection.

83. Le contrôle de l'employeur pourrait intervenir pendant la transmission de la communication. Dans cette hypothèse, nous l'avons vu *supra* l'article 314bis du Code pénal trouve à s'appliquer.

84. Le contrôle pourrait également intervenir après la transmission de la communication, après manipulation spécifique et concertée de l'employé. On peut envisager qu'il soit demandé au destinataire de la communication électronique de procéder lui-même à sa qualification « privée » ou « professionnelle », et de déplacer les courriels privés dans un fichier spécifique. Certes, ceci ne résout pas toute la problématique, car comment mettre à jour et sanctionner le comportement consistant à qualifier abusivement un message de « privé » alors qu'il ne le serait pas par hypothèse ? Quelle attitude avoir face à l'employé paresseux qui ne procède pas au tri qu'il est invité à faire ? Peut-on déduire de cette iner-

⁸⁸ Voy. l'avis 10/2000, p. 6.

tie le consentement visé à l'article 124 de la loi relative aux communications électroniques, celui visé à l'article 314bis du Code pénal ou encore celui visé à l'article 5 de la loi vie privée?

85. Le contrôle est plus délicat encore lorsque le courriel émane d'une personne tierce à l'entreprise puisque la loi exige le consentement de toutes les parties à la communication électronique.

La solution la plus précautionneuse consisterait à exclure les courriels échangés avec des personnes tierces à l'entreprise. Cependant, cette solution ne répond pas adéquatement au souhait de l'employeur de contrôler le travail accompli ou de permettre la poursuite des activités en l'absence du travailleur.

Une solution médiane pourrait être d'aménager le principe de l'exclusion en ajoutant une liste de tiers dont les courriels pourraient faire l'objet d'un contrôle. Par hypothèse, le consentement éclairé de ces tiers aura été sollicité préalablement, par exemple au moment de la conclusion du contrat initial. Le problème est que la mise en place de ce système suppose une structure d'une certaine envergure puisqu'elle comprend et une hiérarchie et une documentation des processus. À cela s'ajoute que la charge de la preuve du consentement est supportée par le responsable du traitement. Or, dans le monde des affaires, il est fréquent que les entreprises ne recourent pas à des contrats écrits. Dans ce contexte, il peut paraître illusoire de recommander à une entreprise la conclusion avec ses partenaires d'un contrat portant sur l'archivage des courriels échangés alors qu'aucun document écrit ne constate l'existence ou les conditions de la prestation principale justifiant le traitement. La prudence recommande donc d'insérer une mention spécifique relative au contrôle des courriels dans le contrat écrit et, à défaut, de renoncer au contrôle.

6) L'exigence de prévision raisonnable

86. La jurisprudence de la Cour européenne des droits de l'homme exige en toute hypothèse que la personne protégée soit avisée du contrôle opéré par l'employeur. À défaut, il faut tenir compte de la prévision raisonnable dans le chef du travailleur du caractère privé de la communication⁸⁹.

7) Le courriel qui a été imprimé

87. L'hypothèse du courriel imprimé intervient nécessairement après la transmission du courriel en sorte qu'il échappe à l'article 314bis du Code pénal. Il

faut en revanche considérer que les dispositions de l'article 124 de la loi relative aux communications électroniques sont applicables.

8) L'archivage informatique

88. La même conclusion que celle du paragraphe précédent s'applique à l'archivage des courriels. Une attention particulière doit cependant être consacrée au fait que le consentement de l'autre partie à la communication peut être requis. De même, l'archivage ne pourrait consister en une mise en copie constante dès lors que cela constituerait une surveillance générale, permanente et *a priori*.

9) Conclusions quant aux correspondances

89. On relève qu'alors que les courriels ne sont pas des lettres au sens de l'article 29 de la Constitution, ils constituent de la correspondance au sens de l'article 8 de la CEDH même lorsqu'ils sont envoyés grâce aux outils mis à la disposition de l'employeur et même lorsque ces outils sont utilisés sur le lieu de l'exécution du travail.

À n'en pas douter, les courriels font l'objet de davantage de protection que les correspondances ordinaires. On peut se poser la question de savoir si ce régime différencié se justifie réellement et, dans l'affirmative, dans quelle mesure il se justifie. Il est vrai que la communication électronique peut facilement faire l'objet d'un traitement – que celui-ci consiste en son transfert, en sa sauvegarde ou en sa suppression. Cependant, il est tout aussi facile de numériser un document qui ne l'était pas au départ et, partant, de jouir des mêmes facilités que dans l'hypothèse où le document avait été numérique dès l'origine.

C. La téléphonie

1) La prise de connaissance des données de trafic

90. Selon une jurisprudence constante de la Cour européenne des droits de l'homme, les données de trafic font partie intégrante des données de communications téléphoniques⁹⁰.

91. À l'occasion de l'examen du projet de loi relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées, le législateur s'est prononcé sur le repérage par l'employeur du numéro formé par l'employé. Il a considéré

⁸⁹ Cour eur. D.H., *Halford c. Royaume-Uni*, 25 juin 1997, Rec., 1997-III, 39, § 45; Cour eur. D.H., *Copland c. Royaume-Uni*, 3 avril 2007, Public. Cour eur. D.H., deuxième section, n° 62617/00; <http://hudoc.echr.coe.int/>, § 42.

⁹⁰ Voy. notamment Cour eur. D.H., *Malone c. Royaume-Uni*, 2 août 1984, n° 8691/79, série A, n° 82, § 84; Cour eur. D.H., *Copland c. Royaume-Uni*, 3 avril 2007, Public. Cour eur. D.H., deuxième section, n° 62617/00; <http://hudoc.echr.coe.int/>, § 43.

qu'il « ne semble pas illégitime qu'un employeur connaisse à tout le moins les numéros de téléphone appelés par son employé à l'étranger, puisque c'est lui qui paiera la facture, laquelle mentionne les numéros en question. En outre, un employé n'est pas censé utiliser le téléphone de son employeur à des fins privées. S'il le fait, il sait que ce dernier recevra la facture et pourra, le cas échéant, demander à Belgacom quels numéros ont été appelés ou, s'il s'agit d'un central numérique, consulter la mémoire de ce central »⁹¹.

92. Le caractère légitime de la démarche a, semble-t-il, convaincu un certain nombre de magistrats qui ont admis la production par l'employeur – en sa qualité d'abonné au service de téléphonie – de factures portant sur les communications électroniques⁹². Cependant, la circonstance que les informations peuvent être obtenues légalement par le biais de relevés téléphoniques ne fait pas obstacle à la constatation d'une violation des droits garantis par l'article 8 de la CEDH⁹³. Il appartiendra au magistrat appelé à connaître de l'affaire d'examiner si l'atteinte au droit au respect de la vie privée au regard de l'article 8 de la Convention européenne des droits de l'homme ou de l'article 22 de la Constitution peut ou non constituer une atteinte légitime.

2) Interception de communications téléphoniques sur le lieu de travail

93. Dans l'arrêt *Halford* du 25 juin 1997, la question posée à la Cour européenne des droits de l'homme est de savoir si les conversations téléphoniques que Madame Halford a eues sur son lieu de travail relèvent ou non des notions de « vie privée » et de « correspondance » au sens de l'article 8 de la CEDH⁹⁴.

En l'espèce, Mme Halford a travaillé dans la police jusqu'à sa retraite en 1992. Elle a été promue, en 1983, contrôleur général de la police de Merseyside (Royaume-Uni). Elle engage en 1990 une procédure à l'encontre de la police et du ministre de l'Intérieur en raison de la discrimination dont elle se prétend victime : à plusieurs reprises, elle n'aurait pas été promue à des postes pourtant vacants alors qu'elle en avait la capacité. Dans le cadre de ses fonctions de contrôleur général, Mme Halford dispose, au bureau, de deux téléphones dont l'un à usage privé et, à son domicile, d'une prise en charge d'une partie importante de ses communications téléphoniques. Mme Halford allègue avoir été victime d'interception de ses appels téléphoniques tant passés depuis son bureau

que depuis son domicile. Selon elle, le but de cette interception serait d'obtenir des informations pouvant être utilisées à son encontre dans le cadre de la procédure en matière de discrimination. Elle réussit à établir que ses communications téléphoniques ont été interceptées.

La Cour fera droit à la demande de Mme Halford dès lors que « les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent se trouver compris dans les notions de « vie privée » et de « correspondance » visées à l'article 8 » de la CEDH⁹⁵.

3) Les communications effectuées par le biais d'un téléphone portable

94. Dans la mesure où les communications réalisées depuis le bureau du travail grâce aux outils de communications mis à sa disposition par l'employeur ne peuvent *a priori* être considérés comme étant des courriers professionnels, il est indubitable qu'il en est également ainsi des communications réalisées grâce à un téléphone portable, par exemple depuis le domicile du travailleur.

95. L'attention est attirée sur la nécessité de mettre en place une politique de sécurité et de protection adéquate notamment dans le cadre de l'usage des *smartphones*. Ces outils permettent d'accéder aisément et rapidement à des données confidentielles, mais aussi à des données à caractère personnel. Afin de prévenir le risque de détournement de ces informations, les travailleurs devraient être invités à prendre toutes les précautions utiles pour s'assurer de leur confidentialité, notamment par le recours à un code de verrouillage après une courte période d'inactivité.

4) Conclusion quant aux communications téléphoniques

96. Les notions de « correspondance » et de « vie privée » au sens de l'article 8 de la CEDH ont une acception large puisqu'elles comprennent notamment les communications téléphoniques. Celles-ci visent tant les données de contenu que les données de trafic. La circonstance que la communication a lieu sur le lieu du travail ou encore qu'elle se fait au moyen d'un outil de communication mis à disposition par l'employeur ne permet pas d'exclure *a priori* le caractère privé de la communication téléphonique envisagée.

D. L'utilisation d'internet

97. Dans le cadre de la navigation sur internet, les données de trafic constituent aussi des données à caractère personnel dès l'instant où l'employeur est en mesure d'établir un lien entre les adresses des sites consultés et un employé

⁹¹ Ann. Parl. Sénat, 1992-1993, n° 843/2, Rapport de la commission de la justice, p. 42.

⁹² Voy. en ce sens Trib. trav. Bruxelles (3^e ch.), 16 septembre 2004, *J.T.T.*, 2005, p. 61; Trib. trav. Liège (5^e ch.), 16 mai 2007, R.G. n° 358-538, *www.cass.be*; C. trav. Liège, 21 mai 2001, *J.T.T.*, 2002, p. 180; C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2002, p. 41.

⁹³ Cour eur. D.H., *Copland c. Royaume-Uni*, 3 avril 2007, *Public. Cour eur. D.H.*, deuxième section, n° 62617/00; *http://hudoc.echr.coe.int/*, § 43.

⁹⁴ Cour eur. D.H., *Halford c. Royaume-Uni*, 25 juin 1997, *Rec.*, 1997-III, 39, § 44.

⁹⁵ *Ibid.* Dans le même sens, Cour eur. D.H., *Amann c. Suisse*, 16 février 2000, *Publ. Cour eur. D.H.*, 2000, II, p. 244, § 43.

particulier. La C.P.V.P. « est d'avis que le contrôle doit se fonder sur des données objectives restreintes et non sur une prise de connaissance préalable et systématique du contenu de toutes les données de trafic concernant chaque employé. L'employeur pourra à cet effet disposer, par exemple, d'une liste d'adresses de sites consultés de façon globale sur une certaine période, sans que soient identifiés dans un premier temps les auteurs des consultations. Il pourra sur cette base repérer une durée anormalement élevée de consultation d'internet ou la mention d'adresses de sites suspects et prendre les mesures de contrôle appropriées. La détection de la consultation de certains sites pourrait également être effectuée de façon automatique grâce à un logiciel spécifique sur la base de mots-clés déterminés »⁹⁶.

98. On se souvient que dans l'affaire *Copland*⁹⁷ précitée l'usage d'internet fait par la requérante avait été l'objet d'une surveillance. Le gouvernement anglais a précisé que la mesure consistait à analyser les sites visités par la requérante, ainsi que le jour, l'heure et la durée de ces visites. À cette occasion, la Cour européenne a considéré que les éléments recueillis au moyen d'une surveillance de l'usage qu'une personne fait d'internet doivent également jouir de la protection de l'article 8 de la CEDH⁹⁸. Elle ajoute que présumer, *a priori*, le caractère privé de la consultation de sites internet est une attente raisonnable⁹⁹.

⁹⁶ Avis 10/2000, p. 7.

⁹⁷ Cour eur. D.H., *Copland c. Royaume-Uni*, 3 avril 2007, *Public*. Cour eur. D.H., deuxième section, n° 62617/00; <http://hudoc.echr.coe.int/>, § 43.

⁹⁸ *Ibid.*, § 41.

⁹⁹ *Ibid.*, § 42. Voy. également C. trav. Bruxelles, 8 avril 2003, *Chr. D. S.*, 2005, pp. 208-214.

E. Tableau récapitulatif des instruments susceptibles de s'appliquer

99. Le tableau qui suit a pour ambition d'aider le praticien à identifier les règles qui trouvent à s'appliquer selon la technologie considérée.

	Correspondance ordinaire	Correspondance électronique	Utilisation d'internet	Utilisation d'un téléphone fixe	Utilisation d'un téléphone portable
Art. 22 de la Constitution – exigence d'une loi	✓	✓	✓	✓	✓
Art. 29 de la Constitution – secret des lettres	x	x	x	x	x
Art. 8 de la CEDH	✓	✓	✓	✓	✓
Régime général*	✓	✓	✓	✓	✓
Art. 314bis du Code pénal	x	✓	✓	✓	✓
Art. 124 de la loi relative aux communications électroniques	x	✓	✓	✓	✓
CCT n° 81	x	✓	✓	✓	✓
Avis 10/2000**	x	✓	✓	x	x
Recommandation 08/2012	x	✓	✓	x	x

* Voy. *supra*, § 72.

** L'avis 10/2000 fait cependant usage récurrent de l'expression « télécommunication », laissant entendre qu'il pourrait s'appliquer à l'usage des téléphones fixes et portables.

Conclusions générales

100. La première partie de cette contribution s'est attachée à examiner le cadre juridique actuel de la vie privée au travail. La critique a porté, pour l'essentiel, sur le caractère complexe de la législation actuelle tant en raison du nombre élevé de dispositions différentes applicables qu'en raison de la difficulté de les concilier. La législation belge présente, de surcroît, une difficulté pratique dès lors qu'elle rend excessivement difficile le traitement de données à caractère personnel.

101. Cette carence législative explique les tentatives du Conseil national du travail et de la C.P.V.P. d'assouplir le système actuel. L'adoption d'une charte d'utilisation des outils de communication au niveau de l'entreprise elle-même participe de la même idée. Elle doit être encouragée ne serait-ce que dans la mesure où elle répond à l'exigence de transparence inhérente à tout traitement de données à caractère personnel. Ces initiatives, aussi louables soient-elles, ne cessent pas d'être selon les cas illégales, nulles ou inconstitutionnelles pour déroger sans base légale au droit à la protection des données à caractère personnel. Cette illégalité est renforcée par les acceptations larges données par la Cour européenne des droits de l'homme aux notions de « correspondance » et de « vie privée ».

102. Une conclusion s'impose à savoir la nécessité de mettre fin à l'insécurité juridique actuelle en adoptant un régime dérogatoire spécifique à la relation de travail.

Bibliographie

- BLANPAIN, R. et VAN GESTEL, M., *Use and Monitoring of E-mail, Intranet and Internet Facilities at Work*, Kluwer Law International, 2004, p. 244.
- BÜLLESBACH, A., GIJRATH, S., POULLET, Y., PRINS, C., *Concise European IT Law*, seconde édition, Law & Business, Wolters Kluwer, 2010.
- CALLEWAERT, J., « La justification du principe de subsidiarité et la charte des droits fondamentaux de l'Union européenne », in *Le principe de subsidiarité*, sous la direction de Fr. Delpérée, Bruxelles, Bruylant, 2002, pp. 349-358.
- DE BARDEMAEKER, R., « Admissibilité d'une preuve illicitement recueillie : quand la fin justifie les moyens... », *J.L.M.B.*, 2009, p. 584.
- DE BARDEMAEKER, R. et KOKOT, M., « Protection de la vie privée et contrat de travail », *J.T.T.*, 2006, pp. 1 à 13.

DE KERCHOVE, G., « La subsidiarité et la charte des droits fondamentaux de l'Union européenne », in *Le principe de subsidiarité*, sous la direction de Fr. Delpérée, Bruxelles, Bruylant, 2002, pp. 335-342.

DUMORTIER, F. et OMRANI, F., « La criminalité informatique », in « Chronique de jurisprudence 2019-2011 », *R.D.T.I.*, n° 48-49/2012, pp. 198-207.

FRUMER, Ph., *La renonciation aux droits et libertés. La Convention européenne des droits de l'homme à l'épreuve de la volonté individuelle*, Bruxelles, Bruylant, ULB, 2001, 646 p.

GILSON, S., LAMBINET, F., ROSIER, K., *Le droit au respect de la vie privée du travailleur. État des lieux*, Limal, Anthemis, CRIDS, 2012, 146 p.

KÉFER, F., « La légalité de la preuve confrontée au droit à la vie privée du salarié », in *La vie privée au travail*, sous la direction de M. Verdussen et P. Joassart, Limal, Anthemis, 2011, pp. 17-58.

LECLERCQ, J.-F. (dir. scientifique), *Vie privée du travailleur et prérogatives patronales*, C.J.B., Édition du jeune barreau de Bruxelles, 2005, p. 239.

LEFEVER, N., « Exécution du contrat de travail à distance : le télétravail », in *Le droit du travail à l'ère numérique*, sous la direction de K. Rosier, Limal, Anthemis, CRIDS, 2011, pp. 121-149.

LUCIANI, M., « La subsidiarité et le rapport entre les ordres juridiques protecteurs des droits fondamentaux », in *Le principe de subsidiarité*, sous la direction de Fr. Delpérée, Bruxelles, Bruylant, 2002, pp. 343-347.

NEVEN, J.-Fr., « Les dispositions internationales et constitutionnelles », in *Vie privée du travailleur et prérogatives patronales*, sous la direction scientifique de J.-F. Leclercq, C.J.B., Édition du jeune barreau de Bruxelles, 2005, pp. 15-53.

OMRANI, F. et VAN GYSEGHEM, J.-M., « Quand le transfert des données "santé" est illégal », Note sous Tribunal de la fonction publique de l'Union européenne (1^{re} ch.), 7 juillet 2011, *R.D.T.I.*, n° 45, Bruxelles, Larcier, pp. 121-149.

PAILLER, L., *Les réseaux sociaux sur internet et le droit au respect de la vie privée*, Bruxelles, Larcier, 2012, p. 210.

ROBERT, R., « Correspondance et vie privée sur les lieux du travail : une cohabitation difficile », *Orientations*, n° 7, sept. 2008, pp. 16-22.

ROSIER, K., « Chronique de jurisprudence (2002-2009) - Droit social : contrôle de l'usage des technologies de l'information et de la communication dans les relations de travail », *R.D.T.I.*, n° 35, pp. 126-140.

VAN OMMESLAGHE, P., *Droit des obligations*, volume I, Bruxelles, Bruylant, 2010.

VAN WASSENHOVE, S., « Le respect de la vie privée dans l'usage des nouvelles technologies », in *Vie privée du travailleur et prérogatives patronales*, sous la direction

scientifique de J.-F. Leclercq, C.J.B., Édition du jeune barreau de Bruxelles, 2005, pp. 139-185.

VERDUSSEN, M., « La protection des droits fondamentaux en Europe : Subsidiarité et circularité », in *Le principe de subsidiarité*, Bruxelles, Bruylant, 2002, pp. 311-333.

VERDUSSEN, M. et JOASSART, P. (dir.), *La vie privée au travail*, Limal, Anthemis, 2011, p. 163.

WÉRY, P., *Droit des obligations*, volume 1, 2^e édition, Bruxelles, Larcier, 2011.

Table des décisions citées

Cour européenne des droits de l'homme

Cour eur. D.H., *Lee Davies c. Belgique*, 28 juillet 2009, *Public. Cour eur. D.H.*, deuxième section, n° 18704/05, <http://hudoc.echr.coe.int/>.

Cour eur. D.H., *Copland c. Royaume-Uni*, 3 avril 2007, *Public. Cour eur. D.H.*, deuxième section, n° 62617/00, <http://hudoc.echr.coe.int/>.

Cour eur. D.H., *Amann c. Suisse*, 16 février 2000, *Publ. Cour eur. D.H.*, 2000, p. 244.

Cour eur. D.H., *Halford c. Royaume-Uni*, 25 juin 1997, *Rec.*, 1997-III, 39.

Cour eur. D.H., *Niemietz c. Allemagne*, 16 décembre 1992, *Public. Cour eur. D.H.*, série A, n° 251.

Cour eur. D.H., *Sunday Times c. Royaume-Uni*, 26 avril 1979, *Public. Cour eur. D.H.*, série A, n° 6538/74, recueil vol. 30, p. 31.

Cour de justice de l'Union européenne

C. J. C. E., 6 novembre 2003, *Lindqvist c. Suède*, *Rec. C.J.C.E.*, 2003, p. I-13014, C-101/01.

Cour constitutionnelle

C.A., 19 juillet 2005, n° 131/2005, *M.B.*, 8 août 2005, pp. 34459-34462.

Cour de cassation

Cass., 1^{er} octobre 2009, n° C.08.0064.N, www.cass.be.

Cass., 10 mars 2008, n° S.07.0073.N, www.cass.be.

Cass., 12 octobre 2005, n° P050119F, www.cass.be.

Cass. (2^e ch.), 2 mars 2005, n° P.04.1644.F, www.cass.be.

Cass. (2^e ch.), 14 octobre 2003, n° P030762N, www.cass.be.

Cass. (2^e ch.), 27 février 2001, n° P.99.0706.N/1, www.cass.be.

Cass., 28 septembre 1979, *Pas.*, 1980, I, p. 131.

Cass., 10 novembre 1978, *Pas.*, 1979, I, p. 309.

Cass., 2 mai 1969, *Pas.*, 1969, I, p. 781.

Cass., 15 mars 1968, *Pas.*, 1968, I, p. 894.

Cass., 9 décembre 1948, *Pas.*, I, p. 699.

Cass., 12 mars 1923, *Pas.*, 1923, I, pp. 233 et 234.

Cours du travail

C. trav. Bruxelles (2^e ch.), 7 février 2013, n° 2012/AB/1115, <http://jure.juridat.just.fgov.be/>.

C. trav. Liège, 8 mars 2011, *Chron. D.S.*, 2011, p. 404.

C. trav. Mons, 8 décembre 2010, *Chron. D.S.*, 2011, p. 399.

C. trav. Anvers (sect. Hasselt), 2 septembre 2008, *Orientations*, 2009, p. 22, note K. ROSIER.

C. trav. Bruxelles, 15 juin 2006, R.G. n° 48484, <http://jure.juridat.just.fgov.be/>.

C. trav. Bruxelles, 3 mai 2006, *J.T.T.*, 2006, p. 262.

C. trav. Bruxelles, 13 septembre 2005, *Computerr.*, 2006, p. 100.

C. trav. Anvers (sect. d'Anvers), 15 décembre 2004, *Chr. D. S.*, 2006, p. 146.

C. trav. Liège, 17 mai 1985, *J.T.T.*, p. 472.

C. trav. Bruxelles (3^e ch.), 10 février 2004, *Orientatie*, 2004, p. 3.

C. trav. Anvers (sect. Anvers), 1^{er} octobre 2003, *J.T.T.*, 2004, p. 510.

C. trav. Bruxelles, 8 avril 2003, *Chr. D. S.*, 2005, pp. 208-214.

C. trav. Liège (sect. Namur), 25 avril 2002, www.cass.be.

C. trav. Gand, 22 octobre 2001, *J.T.T.*, 2002, p. 41.

C. trav. Liège, 21 mai 2001, *J.T.T.*, 2002, p. 180.

C. trav. Gand, 4 avril 2001, *J.T.T.*, 2002, p. 49.

C. trav. Liège, 25 avril 2004, www.cass.be.

Cours d'appel

Liège, 22 novembre 1979, *Jur. Lg.*, 1980, p. 1.

Tribunaux du travail

Trib. trav. Liège (3^e ch.), 3 septembre 2008, R.G. n° 371 .015, www.cass.be.

- Trib. trav. Liège (3^e ch.), 19 mars 2008, R.G. n° 360 .454, www.cass.be.
Trib. trav. Bruxelles, 4 décembre 2007, *J.T.T.* 2008, n° 1005, p. 179.
Trib. trav. Liège (5^e ch.), 16 mai 2007, R.G. n° 358 .538, www.cass.be.
Trib. trav. Bruxelles (3^e ch.), 16 septembre 2004, *J.T.T.*, 2005, p. 61.
Trib. trav. Hasselt (1^{re} ch.) 21 octobre 2002, *Chron. D. S.*, 2004, p. 197.
Trib. trav. Verviers (1^{re} ch.), 20 mars 2002, *J.T.T.*, 2002, p. 183.
Trib. trav. Gent, 4 avril 2001, *J.T.T.*, 3/2002, pp. 49-52.
Trib. trav. Bruxelles, 2 mai 2000, *Computerr.*, 2001, p. 26, note D. CASAER.