La protection de la vie privée au travail

Conférence du Jeune Barreau de Luxembourg

Auditoire BG BNP Paribas

28 février 2014

Gérard Lommel

Président

Résumé

- Introduction
- Récapitulatif des principaux textes applicables
- Définitions et notions essentielles
- Les grands principes de la protection des données
- Les notions de droit à la vie privée, à la protection des données personnelles et la relation de travail
- Les traitements de données à des fins de surveillance: Distinction entre le régime général et le régime spécifique de la surveillance sur le lieu de travail
- Analyse des cas pratiques
  - Vidéosurveillance
  - Enregistrement des conversations téléphoniques
  - Dispositifs de géolocalisation
  - Contrôle de l'utilisation des outils informatiques
  - Systèmes de reconnaissance biométrique

Récapitulatif des principaux textes applicables

- Les textes internationaux
  - Convention de sauvegarde des droits de l'homme et des libertés fondamentales (Rome, 4 novembre 1950)
  - Convention 108 (Strasbourg, 28 janvier 1981)
  - Charte des droits fondamentaux de l'Union Européenne (Nice,7 décembre 2000 intégrée au Traité de Lisbonne de 2008)
  - Directive 95/46/CE du 28/10/1995 (« protection des données »)
  - Directive 2002/58/CE («vie privée et communications électroniques»)
  - Directives 2006/24/CE et 2009/136/CE (modifiant la précédente)
- Les textes luxembourgeois
  - Loi-cadre modifiée du 2 août 2002 (relative à la protection des personnes à l'égard du traitement des données à caractère personnel)
  - Loi du 30 mai 2005 (protection des données et communications électroniques) modifiée par les lois du…2010 et …2011)
  - Loi du 11 août 1982 (protection de la vie privée)

Convention de sauvegarde des droits de l'homme et des libertés fondamentales (Rome, 1950)

- **Article 8 – Droit au respect de la vie privée et familiale**
  1. *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*
  2. *Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

Charte des droits fondamentaux de l'Union Européenne (2000)

- **Article 7 - Respect de la vie privée et familiale**
  - *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de ses communications. »*
- **Article 8 - Protection des données à caractère personnel**
  1. *« Toute personne a droit à la protection des données à caractère personnel la concernant.*
  2. *Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.*
  3. *Le respect de ces règles est soumis au contrôle d'une autorité indépendante. »*

Définitions et notions essentielles

- **Donnée à caractère personnel** – (article 2 lettre (e))
  - *« Toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, concernant une personne identifiée ou identifiable (personne concernée) ».*
  - Cf. considérant 26 de la directive :

    « pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre, soit par le responsable du traitement, soit par une autre personne, pour identifier ladite personne; que les principes de la protection ne s'appliquent pas aux données rendues anonymes d'une manière telle que la personne concernée n'est plus identifiable. »

Définitions et notions essentielles

- **Responsable du traitement et sous-traitant**– définition (article 2, lettre (n)et (o))
  - Responsable du traitement

    «*la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel. Lorsque les finalités et les moyens du traitement sont déterminés par ou en vertu des dispositions légales, le responsable du traitement est déterminé par ou en vertu des critères spécifiques conformément aux dispositions légales »*
  - *sous-traitant:*

    « la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des données pour le compte du responsable du traitement »
- **Personne concernée** – définition (article 2, lettre (m))

  « toute personne physique (…) qui fait l'objet d'un traitement de données à caractère personne. »

Définitions et notions essentielles

- **Surveillance** – définition (article 2, lettre (p))
  - « *Toute activité qui, opérée au moyen d'instruments techniques, consiste en l'observation, la collecte ou l'enregistrement de manière non occasionnelle des données à caractère personnel d'une ou de plusieurs personnes, relatives à des comportements, des mouvements, des communications ou à l'utilisation d'appareils électroniques et informatisés* ».

Les grands principes de la protection des données

1. L'exigence d'un critère de légitimation

- Idée : Autodétermination informationnelle ou fondement légal justifiant le traitement *(Charte)*,
- *L'intérêt de l'acteur est à soumettre au test de mise en balance avec les droits des personnes*
- Différenciation régime général et régime dérogatoire.
  - **Régime général** (article 5 loi de 2002) applicable à tout traitement de données
  - **Régime dérogatoire** : s'applique qu'aux traitements à des fins de surveillance (articles 10 et 11 nouveau de la loi de 2002), énumération limitative

Les grands principes de la protection des données

- **Art. 5. Légitimité du traitement**
  - *«(1) Le traitement de données ne peut être effectué que (...):*
    - *(a) s'il (…) est nécessaire au **respect d'une obligation légale** à laquelle le responsable du traitement est soumis, ou*
    - *(b) s'il (…) est nécessaire 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 ou les tiers auxquels les données sont communiquées, ou*
    - *(c) s'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, ou*
    - *(d) s'il (…) est nécessaire à la **réalisation de l'intérêt légitime** poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er, ou*
    - *(e) s'il (…) est nécessaire à la **sauvegarde de l'intérêt vital** de la personne concernée, ou*
    - *(f) si la personne concernée a donné son **consentement**.»*

Les grands principes de la protection des données

2. Qualité des données et loyauté du traitement

- Art. 4. Qualité des données
  - *« (1) Le responsable du traitement doit s'assurer que les données qu'il traite le sont loyalement et licitement, et notamment que ces données sont:*
    - *(a) collectées pour des **finalités déterminées, explicites et légitimes**, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités;*
    - *(b) **adéquates, pertinentes et non excessives au regard des finalités** pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement;*
    - *(c) **exactes et, si nécessaire, mises à jour**; toute mesure raisonnable doit être prise pour que les données inexactes ou incomplètes, au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement, soient effacées ou rectifiées;*
    - *(d) **conservées** sous une forme permettant l'identification des personnes concernées **pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités** pour lesquelles elles sont collectées et traitées (…).*

Les grands principes de la protection des données

- **Principe de finalité -** Art. 4 (1) (a)
  - Tout traitement de données poursuit par nature un certain but
  - Cet ou ces objectifs poursuivis doivent être clairement spécifiés
  - Permet de déterminer concrètement les données, destinataires et opérations justifiées pour l'atteindre et d'en circonscrire les limites exactes
  - → éviter les détournements de finalité
  - ***Cour d'Appel Versailles 3 mars 2003***: *« les besoins de la défense de la société X devant les prud'hommes ne peuvent pas excuser le fait d'avoir commis sciemment ce détournement de finalité ».* (voir aussi: ***TGI Rennes 8 décembre 1988 ; TGI Paris 16 décembre 1994, TGI Paris 25 avril 2003, société Sonacotra / Syndicat SUD***)
  - → traitement ultérieur interdit pour des finalités **incompatibles** avec la finalité affichée initialement ou à laquelle il a été consenti (ce qui dépasse la prévisibilité des personnes concernés

Les grands principes de la protection des données

- **Principes de nécessité et de proportionnalité**

Article 4 (1) (b): jurisprudence Mister Minit /c. CNPD

- **Nécessité** :
  - ***Trib. Adm., 15 décembre 2004, n°17890 :*** *« En effet, un dispositif dont la mise en place peut paraître opportune à de multiples égards – diminution du risque de vol par l'effet dissuasif des caméras par exemple – n'est pas pour autant à considérer automatiquement comme étant nécessaire, la nécessité excédant en effet la simple opportunité en ce sens qu'elle vise ce dont on a absolument besoin, dont on ne peut se passer, l'indispensable, soit quelque chose qui va au-delà de ce qui simplement convient au temps, au lieu, aux circonstances et qui caractérise le simplement opportun »**. Confirmé par **Cour Adm., 12 juillet 2005, n°19234C.***
- **Proportionnalité** :
  - ***Cour Adm., 12 juillet 2005, n°19234C*** : *« Afin d'être en mesure d'assurer la mission qui lui est ainsi conférée par le législateur, la CNPD doit nécessairement procéder à un contrôle de la proportionnalité des mesures envisagées pour décider si le traitement ainsi préconisé est nécessaire pour assurer les besoins prévus par la loi. Partant, loin d'avoir dépassé ses compétences légales, la CNPD a agi conformément à la mission lui conférée par le législateur, tel que cela a été retenu à bon droit par les premiers juges. »*

Les grands principes de la protection des données

- **Principe de transparence**
  - Obligation d'information
  - Pas de surveillance cachée
- Corollaires
  - **Principe d'exactitude des données** Art. 4 (1) (c)
    - Données doivent être exactes et mises à jour.
    - Données inexactes ou incomplètes doivent être effacées ou rectifiées
  - **Durée de conservation limitée -** Art. 4 (1) (d)
    - Anonymisation possible (si irréversible)
    - Survenance d'un « incident »
  - **Obligation de prendre les mesures appropriées pour garantir la confidentialité et la sécurité des données**
  - **-** Art.'s 21 à 23

Les notions de droit à la vie privée, à la protection des données personnelles et la relation de travail

- Jurisprudence: Vie privée au travail et relation d'emploi (lien de subordination)

  - ***CEDH, Niemietz c. Allemagne, 16.12.1992:*** *« 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 »*.
  - ***CEDH, Copland c. Royaume-Uni, 3.04.2007:*** Faute de notice d'information préalable quant à la possibilité d'un contrôle, la salariée pouvait avoir une espérance légitime quant au caractère privé de ses communications. Violation de l'article 8.
  - ***CEDH, Halford c. Royaume-Uni, 27.07.1997*** : *« 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 par. 1 (art. 8-1) »*.
  - ***CEDH, Peev c. Bulgarie, 26.07.2007*** : En se basant sur les décisions de ***CEDH, Chappell c. Royaume-Uni, 30 mars 1989 ; Niemietz, précité ; CEDH, Funke c. France, 25 février 1993 et CEDH, Crémieux c. France, 25 février 1993***, qui ont consacré la position que *« une perquisition effectuée dans un local professionnel ou dans le bureau d'une personne exerçant une profession libérale s'analysait en une atteinte au droit au respect non seulement de la vie privée mais aussi du domicile de l'intéressé »*.

Les traitements de données à des fins de surveillance:

Distinction entre le régime général et le régime spécifique de la surveillance sur le lieu de travail

- Volonté du législateur:
  - Éviter prolifération des dispositifs de surveillance
  - Garantir la sécurité juridique pour tous les acteurs
- Régime particulièrement protecteur:
  - Instauration d'un catalogue limitatif des conditions de légitimité dérogeant à la liste de l'article 5 (Art. 7 de la directive)
  - Exigence d'autorisation préalable auprès de la CNPD contrôle a priori par application des considérants 53 et 54 de la directive
- Articulation des textes applicables:
  - **L'article L.261-1 du Code du Travail** (article 11 nouveau de la loi) s'applique aux seules situations d'une surveillance des salariés mise en œuvre par l'employeur sur le lieu du travail
  - **L'article 10** s'applique à tous les autres cas dans lesquels une surveillance est mise en oeuvre

Article 10- Traitement à des fins de surveillance

- *« (1) Le traitement à des fins de surveillance ne peut être effectué que:*
  - *(a) si la personne concernée a donné **son consentement**, ou*
  - *(b) **aux abords ou dans tout lieu** accessible ou non au public **autres que les locaux d'habitation**, notamment dans les parkings couverts, les gares, aérogares et les moyens de transports publics, pourvu que le lieu en question **présente de par sa nature, sa situation, sa configuration ou sa fréquentation un risque rendant le traitement nécessaire**:*
    - *«-**à la sécurité des usagers ainsi qu'à la prévention des accidents**;(...)*
    - *-**à la protection des biens**, s'il existe un risque caractérisé de vol ou de vandalisme», ou*
  - *(c) **aux lieux d'accès privé** dont la personne physique ou morale y domiciliée est le responsable du traitement, «ou»*
  - *(d) si le traitement est n**écessaire à la sauvegarde des intérêts vitaux** de la personne concernée ou d'une autre personne dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement*. »

Article 10- Traitement à des fins de surveillance

- **Régime général**
  - applicable à toutes les situations en dehors du contexte de l'emploi.
  - nécessaire de l'intégrer ici, car l'article 10 et l'article L. 261-1 susceptibles de s'appliquer en même temps.
- **Obligation d'information renforcée**
- Autorisation préalable exigée uniquement si les données /images/sons **font l'objet d'un enregistrement**
- **Conservation, transmission limitées,** possible à la police et aux autorités judiciaires
- Loi **ne s'applique pas** *« au traitement mis en œuvre par une personne physique dans le cadre exclusif de ses **activités personnelles ou domestiques**»*,
  - Attention : interprétation restrictive → dès qu'un salarié est susceptible de passer dans le champ de vision de la caméra, l'exception de l'article 3 § (3) (champ d'application) ne joue plus.

Article 11 – Traitement à des fins de surveillance des salariés sur le lieu de travail

- L'article 11 nouveau de la loi fait un **renvoi à l'article L.261-1 du Code du Travail** :
  - *« (1) Le traitement des données à caractère personnel à des fins de surveillance sur le lieu de travail peut être mis en œuvre, conformément à l'article 14 de la loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, par l'employeur s'il en est le responsable. Un tel traitement n'est possible que s'il est nécessaire:*
    1. *pour les besoins de **sécurité et de santé des salariés**, ou*
    2. *pour les besoins de **protection des biens de l'entreprise**, ou*
    3. *pour le **contrôle du processus de production portant uniquement sur les machines**, ou*
    4. *pour le **contrôle temporaire de production ou des prestations du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact**, ou*
    5. *dans le cadre d'une **organisation de travail selon l'horaire mobile** conformément au présent code. »*

Article 11 – Traitement à des fins de surveillance des salariés sur le lieu de travail

- Présence d'un **lien de subordination**
  - *« Pour qu'il y ait rapport de subordination juridique, il faut que le contrat place le salarié sous l'autorité de son employeur qui lui donne des ordres concernant la prestation du travail, en contrôle l'accomplissement et en vérifie les résultats »*.
    - Source: Le Contrat de Travail – Droit et Jurisprudence, R. Schintgen et J.Faber, Publication du Ministère du Travail et de l'Emploi, janvier 2010, p. 16. Y sont cités : ***Cour 1er février 1978, Scheidtweiler c/ Express SA; Cour 21 décembre 1989, Gillain c/ Flebus et Laroire ; Cour 14 mai 1993, Wassermann c/ Transcomerz ; Cour 9 janvier 1997, Parravano c/ Winlux SA***.
- **Pouvoir décisionnel du comité mixte**
  - Sécurité/santé, contrôle temporaire et horaire mobile.
- Le **consentement est inopérant** pour les salariés
- Obligation d'**information étendue** (Comité mixte, délégation, sinon ITM)

Contrôle a priori – formalités

- **L'article 14** soumet à l'autorisation de la CNPD toute forme de surveillance (définition, personnes identifiables)
  - Exception: surveillance art. 10 (tiers) sans enregistrement
  - La jurisprudence sanctionnant l'absence de demande d'autorisation est abondante: ***TA 21 octobre 2010, n°3429/2010 ; TA 27 octobre 2008, n°3055/2008 ; TA 24 avril 2008, n°1342/2008***.
- **Régime « allégé »** de l'engagement formel de conformité (contrôle d'accès, horaire mobile)
- Les délibérations de la CNPD sont assorties de **conditions et de restrictions**
  - En vertu du pouvoir d'appréciation de la nécessité/proportionnalité, confirmé en jurisprudence
- Vérifient durée de conservation, Mesures de **sécurité**

Vidéosurveillance

- **Critères de légitimité** admis :
  - L.261-1 (1), L.261-1 (2) et L.261-1 (3).
  - 10 (1)(b) tiret 1 ou 2, 10(1)(c) et 10(1)(c).
- **Application conjointe** art 10 et L.261-1 possible.
- Durée de **conservation** : 7 jours, SAUF justification spéciale : 15-30 jours.
- N.b.: La surveillance de la voie publique en vue de la prévention de la délinquance et de la constatation d'infractions pénales est régie par l'art 17. (Traitements de la Police: autorisation par voie réglementaire, p.ex. Visupol)
- **Applications jurisprudentielles**:
  - VS ne doit être jamais permanente et jamais cachée.
  - Pas VS à l'insu : ***TA 24 avril 2008, n°1342/2008***, tous secteurs concernés.
  - Problème de la **loyauté de la preuve: du procès équitable**

Admissibilité d'une preuve illicite

- C.Cass. Lux, 22 novembre 2007, n°57/2007:pénal

Condition fondamentale du respect de la légalité dans l'administration de la preuve ;

- « le juge ne peut écarter une preuve obtenue illicitement que si le respect de certaines conditions de forme est prescrit à peine de nullité, si l'irrégularité commise a entaché la crédibilité de la preuve ou si l'usage de la preuve est contraire au droit à un procès équitable ; …
  - Qu'il appartient néanmoins au juge d'apprécier l'admissibilité d'une preuve obtenue illicitement en tenant compte des éléments de la cause prise dans son ensemble y compris le mode d'obtention »

Admissibilité d'une preuve illicite

- **C.App. Lux, 26 février 2008.** : la Cour d'Appel de renvoi estime qu'il y a violation du droit à un procès équitable qui ne résulte pas exclusivement du fait que le système de vidéosurveillance n'a pas été autorisé par la CNPD, mais elle prend aussi en considération le non-respect de certaines dispositions du code d'instruction criminelle quant au repérage de données au moyens de télécommunication. Elle conclut que « *dans les conditions données, et alors que de la combinaison de la production en justice d'un moyen de preuve illicite et d'une procédure qui elle-même n'est pas conforme aux conforme aux dispositions régissant l'exercice de l'action publique et l'instruction, il résulte en l'espèce une atteinte au droit à un procès équitable…*»

Vidéosurveillance

- L'analyse de la nécessité et de la proportionnalité se fait **par zones** et au cas par cas.
  - Exemples relatifs à la surveillance d'une caisse enregistreuse d'un/d'une:
    - comptoir de vente d'un magasin de détail
    - comptoir d'un restaurant
    - ensemble avec le comptoir de consommation dans une friterie
    - supermarché
    - station de service

Vidéosurveillance

- **Zones généralement acceptées:**
  - Accès
  - Stock de marchandises/réserves/stocks/entrepôts
  - Locaux de transport de fonds
  - Galerie marchande/espace ou surfaces de vente
  - Ascenseurs
  - Parking
  - Sorties de secours
  - Livraisons/chargement
  - Salle informatique/serveurs
  - Car-wash
  - Coffre-fort
  - Etc.

- **Zones généralement refusées :**
  - Bureaux
  - Salle de réunion
  - Salle de repos du personnel
  - Salle de sport
  - Salle de séjour/repos
  - Toilettes
  - Bureau de la représentation du personnel (intérieur)
  - Vestiaire/salle des casiers
  - Salle de consommation/ coin café et petite restauration
  - Etc.
- Solution : les caméras surveillant les accès à ces salles seraient, pour la plupart acceptées.
- **Autres zones refusées :**
  - Intérieur de la cuisine d'un restaurant
  - L'atelier
  - Etc.

Vidéosurveillance

- Notion de **« surveillance permanente »**
  - Zone avec coffre-fort
  - Surface de vente
  - Stock/réserve/entrepôt
  - Guichet de banque
  - Accueil/réception

Enregistrements téléphoniques

- Evolution législative: secret des lettres → secret des communications électroniques
- Application de la loi modifiée du 2 août ET de la loi modifiée du 30 mai 2005.
- Critères de légitimité admis : L.261-1 (2), 10 (1)(a), Art. 4, paragraphe 3, lettre (d), Application conjointe des 3 articles.
- Enregistrements ne sont possibles que s'ils sont effectués aux fins de **« fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale »**.
- Obligation d'information préalable obligatoire « des parties aux transactions », sous réserve de nullité de la preuve.
  - ***C.A. Luxembourg, 24 octobre 2002, no 25235 du rôle, BIJ 2002, p.39 :*** *« Il y a lieu de constater que le tribunal du travail a à juste titre, et pour des motifs que la Cour d'appel adopte, rejeté comme mode de preuve l'enregistrement sur bande magnétique effectué à l'insu de l'une des parties ».* Donc si le dispositif est connu, l'employeur peut contrôler, en ce sens v. ***C.A. Luxembourg, 16 mai 2002, no 25801 du rôle*** *:* L'employeur a le droit de contrôler et de surveiller l'activité de son personnel durant le temps de travail par un dispositif connu,
- Proportionnalité :
  - pas de surveillance du comportement et des performances des salariés.
  - L'employeur doit aussi mettre à disposition des salariés et des correspondants tiers une ligne téléphonique non surveillée.

Enregistrements téléphoniques: sélection de la jurisprudence

- **CEDH, Halford c. Royaume-Uni, 25 juin 1997** : *« … 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 § 1 »*. Dans le même sens : **CEDH, Copland c. Royaume-Uni, 3 avril 2007.**
- **(FR) C.Cass soc., 20 novembre 1991 :** *Si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, tout enregistrement, quel que soit l'activité de ses salariés, quels que soient les motifs, d'images ou de paroles à leur insu constitue un mode de preuve illicite.*
- **(FR) CA Paris 2 novembre 1995 n° 94-37029, 22e ch. C, Sté Crédit commercial de France c/ Fournier** : *L'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail ; seul l'emploi d'un procédé clandestin de surveillance est illicite*.
- **(FR) Cass. soc. 14 mars 2000 n° 98-42.090, Dujardin c/ Sté Instinet France** : *Licéité de la preuve résultant d'un enregistrement des conversations téléphoniques du salarié dès lors que ce dernier était informé de l'existence de ce dispositif*.
- **(FR) Cass. 2e civ., 7 octobre 2004, no 03-12.653** : *L'enregistrement d'une conversation téléphonique privée, effectuée et conservée à l'insu de l'auteur des propos invoqués, est un procédé de preuve déloyal rendant irrecevable en justice la preuve ainsi obtenue*.
- **Solution inverse pour les SMS : (FR) Cass. Chambre sociale, 23 mai 2007** : *Si l'enregistrement d'une conversation téléphonique privée, effectué à l'insu de l'auteur des propos invoqués, est un procédé déloyal rendant irrecevable en justice la preuve ainsi obtenue, il n'en est pas de même de l'utilisation par le destinataire des messages écrits téléphoniquement adressés, dits S.M.S., dont l'auteur ne peut ignorer qu'ils sont enregistrés par l'appareil récepteur*.
- **Précisions quant à l'étendue de l'obligation d'information : (FR) CA Metz 27 juin 2007 n° 04-3854, ch. soc., SARL Arvato services Bertelsmann c/ Heberle** : *Dès lors que le salarié reconnaît avoir été préalablement informé de l'existence du dispositif d'écoute des conversations téléphoniques entretenues par les salariés avec les clients de la société, il importe peu que l'intéressé n'ait pas eu connaissance, ainsi qu'il le soutient, que ces écoutes pourraient être utilisées comme moyens de preuve dans une procédure visant à sanctionner son comportement. Il importe également peu, sauf à les vider de tout sens, que le salarié n'ait pas été prévenu du moment choisi par l'employeur pour mettre en œuvre ces moyens de contrôle*.
- **(FR) Cass. soc. 16 décembre 2008 n° 07-43.993, Pontais c/ Caisse d'épargne de Basse-Normandie** : *L'écoute d'une communication téléphonique réalisée par une partie à l'insu de son auteur constitue un procédé déloyal rendant irrecevable sa production à titre de preuve*.

Dispositifs de géolocalisation

- Les **dispositifs de géolocalisation du véhicule professionnel** sont de plus en plus fréquents
  - fonctionnalités nouvelles: possibilité de détecter la perte de verticalité
- **Interprétation restrictive de la CNPD**, au cas par cas.
- **Critères de légitimité** admis :
  - L.261-1 (1) [sécu/santé] : admis en fonction de la nature des activités, cf. transports de fonds, possibilité d'atteinte à l'intégrité)
  - L.261-1 (2) [Protection des biens] : communément admis
  - L.261-1 (3) [Processus de production portant sur les machines] – interprétation large de la CNPD : la surveillance du salarié doit être subsidiaire, le but étant le contrôle de l'infrastructure matérielle et l'optimisation de son exploitation. Le salarié n'est qu'un accessoire, mais l'objectif de suivre les prestations de service.
  - L.261-1 (5) [Horaire mobile] : admis uniquement si un système d'horaire mobile est effectivement présent en entreprise, avec des créneaux horaires prédéfinis, etc.

Dispositifs de géolocalisation

- Particularités :
  - L'employeur **ne peut pas traiter les données d'excès de vitesse** MAIS il peut traiter : données de géolocalisation (positionnement et itinéraires), données complémentaires telles que date, durée d'utilisation du véhicule, temps de conduite, kilométrage parcouru, heures de début et fin d'activité, etc.
  - Différenciation entre les **véhicules professionnels à usage privé et les véhicules purement professionnels**.
- Durée de **conservation** :
  - Distinction entre
    - les données de localisation (2 mois),
    - les données relatives au temps de travail (3 ans - art 2277 Code civil) et
    - les paramètres purement techniques (kilométrage - hypothèse d'une réidentification possible) : 2 mois, mais conservation au-delà si données anonymisées.

Surveillance des outils informatiques

- Critères de **légitimité** admis :
  - L.261-1 (2) – que protection des biens
  - 10 (1)(a) – exclusivement consentement si surveillance de tiers
- **Application conjointe** art 10 et L.261-1 est possible.
- Durée de **conservation** : 6 mois
  - Ne concerne pas les documents commerciaux et comptables
- Différenciation courrier électronique, utilisation Internet et supports informatiques
- ***CEDH, Niemietz c. Allemagne, 16.12.1992*** (vie privée) et ***CEDH, Copland, 3 avril 2007***: « *La Cour estime dès lors que la collecte et la conservation, à l'insu de la requérante, de données à caractère personnel se rapportant à l'usage qu'elle faisait du téléphone, du courrier électronique et de l'Internet ont constitué une ingérence dans l'exercice du droit de l'intéressée au respect de sa vie privée et de sa correspondance, au sens de l'article 8.* »

Courrier électronique

- Applicabilité du principe du respect de la vie privée et secret des correspondances qui s'applique au courrier personnel et professionnel
  - ***(FR), Cour de Cass., Chambre sociale, 2 octobre 2001, Nikon***: la Cour a constaté que *« le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances »*. L'employeur ne peut donc pas *« prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur »*.
  - ***(FR), Cour de Cass., Chambre sociale, 17 mai 2005, Cathnet-Science***: l'employeur ne peut ouvrir les dossiers d'un salarié contenus sur le disque dur de son ordinateur et identifiés par lui comme personnels, en son absence ou sans l'avoir « dûment appelé ».

Courrier électronique

«La Cour relève qu'il est de principe que le salarié a droit, même au temps et au lieu de travail, au respect de sa vie privée qui implique en particulier le secret de la correspondance dont font partie les courriers électroniques reçus par lui grâce à un outil informatique mis à sa disposition pour son travail.

Le secret des correspondances visé à l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales s'applique dès lors également aux technologies nouvelles de transmission de la correspondance, peu importe l'endroit à partir duquel le courrier électronique est envoyé et réceptionné, de sorte que l'employeur ne peut prendre une connaissance concrète et exacte du contenu des courriers électroniques protégés par le secret de la correspondance.»

Sur base de ces principes, la Cour tranche comme suit : *« Le salarié les ayant identifiés comme personnels (les emails), l'employeur n'est pas autorisé à s'en prévaloir sans l'autorisation du salarié. »*

Courrier électronique

- ***(BE), Cour de Cass., 1er octobre 2009*: la loi exclut « *la prise de connaissance intentionnelle de l'existence d'un courriel, ainsi que l'usage de cette connaissance ou de l'information qui est ainsi obtenue intentionnellement ou non, par quiconque n'y a pas été autorisé au préalable.*»**
- ***(BE), Cour du Travail, 7 février 2013 :* « *L'ingérence de la société appelante dans les courriels privés de Monsieur M., à l'insu de celui-ci et en l'absence de règles déterminées, est établie ; elle viole les principes et les dispositions légales rappelés plus haut relatifs au respect de la vie privée, au secret des communications électroniques. Dans ces conditions les courriels invoqués comme éléments de preuve à l'appui des faits reprochés à Monsieur M. sont manifestement entachés d'irrégularité.* »**
- ***(FR), Cass, chambre sociale, 26 juin 2012, Helpevia***: l'employeur n'avait pas le droit de procéder à la consultation des e-mails en cause (dans le cadre d'un licenciement), alors même qu'ils n'étaient *pas* marqués comme personnels, mais que le règlement intérieur de l'entreprise prévoyait que la direction ne pouvait consulter les messageries électroniques des salariés qu'en présence des salariés.
- ***(FR), Cass, chambre sociale, 18 octobre 2011***, relatif à un courriel relevant de la vie amoureuse d'un salarié: Dans l'hypothèse ou un courrier n'est pas marqué comme personnel et que l'on décèle néanmoins que le courrier est de nature privée ou personnelle, le courriel ne peut pas, du moins dans certains cas, être utilisé en justice par l'employeur.

Courrier électronique

- Mise en œuvre d'une mesure de surveillance et recommandations :
  - Mise en place d'une double boîte de messagerie (pro et privée) au travail.
  - Marquage et sensibilisation au marquage de mails personnels.
  - Recommandations en cas d'absence/départ du salarié.
- Graduation dans la surveillance du courrier électronique

Validité de la preuve en l'absence d'une autorisation préalable de la CNPD

:

Tribunal du travail de Luxembourg, 7 mars 2013:

- Dans une affaire de licenciement, l'employeur verse *« un nombre important de courriers électroniques dont certains figurent en annexe de la lettre de licenciement. »* alors qu'il n'a procédé à aucune demande d'autorisation auprès de la CNPD.
- Le tribunal estime que: *« le fait d'enregistrer ces données de manière non occasionnelle et d'en déterminer le comportement du salarié est à qualifier de surveillance au sens de l'article 2 de la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel. Ainsi, le traitement des données à caractère personnel à des fins de surveillance sur le lieu de travail ne peut être mis en œuvre que conformément à la loi précitée et à l'article 261-1 du code du travail. »* Le tribunal écarte les e-mails en cause des débats.

Tribunal d'arrondissement de Luxembourg, 25 mai 2012, n°874/2012,

- L'employeur verse comme pièces un certain nombre d'e-mails. Il s'estime en droit de les produire puisqu'il ne s'agirait pas d'e-mails privés.
- Le tribunal précise que la loi de 2002 et l'article 261-1 du Code du travail s'appliquent bel et bien aux e-mails professionnels et estime qu'il y a eu en l'espèce une surveillance au sens de la loi. Il rejette les mails en argumentant que l'employeur *« ne rapportant pas la preuve, et n'alléguant même pas, que cette surveillance ait été faite en conformité avec le Code du travail, dont notamment l'information préalable du salarié. »*

Utilisation d'Internet

- Le **principe de la confidentialité des communications électroniques** englobe le recoures à l'internet (article 5 directive vie privée et communications élec).
- Mais l'accès à internet est censé être donné **pour l'utilisation professionnelle**. L'utilisation d'internet à des fins privées peut être interdit ou limité et un contrôle par l'employeur doit donc être possible dans certaines conditions.
  - ***(FR), Cass, chambre sociale, 9 juillet 2008***: «*les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel, de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence*».
  - ***(FR), Cass, chambre sociale, 9 février 2010***: le fait qu'un site se trouve dans les favoris de l'ordinateur professionnel du salarié n'y change rien, « *l'inscription d'un site sur la liste des "favoris" de l'ordinateur ne lui conférant aucun caractère personnel* ».
- **Mise en œuvre d'une mesure de surveillance** :
  - Information obligatoire spécifique de chaque salarié au moyen d'une charte informatique, d'une police ou d'une clause contractuelle.
  - Le contrôle doit être effectué de manière non individualisé (contrôle d'une liste d'adresses de sites consultés), càd pas par identification du salarié. Ce n'est que si la durée de consultation est anormale ou si des adresses consultées sont suspectes, on peut prévoir une 2e phase de surveillance individualisée.
- **Recommandations** : Protection préventive par blocage, suivant URL, listes noires, mots-clés, etc.

Supports informatiques et fichiers de journalisation

- Les dossiers et fichiers sauvegardés sur un outil informatique professionnel sont présumés revêtir un caractère professionnel.Exception : quand ces fichiers sont marqués ou identifiés comme personnels.
  - Voir ***(FR), Cour de Cass., Chambre sociale, 17 mai 2005, Cathnet-Science*** et ***Cour de Cass., Chambre sociale, 21 octobre 2009*** et ***(FR), Cour de Cass., Chambre sociale,10 mai 2012***. :
  - ***(FR), Cour de Cass., Chambre sociale, 13 juin 2013*** **:** Des courriels échangés par le biais d'une messagerie personnelle du salarié sont enregistrés sur le disque dur de l'ordinateur par le salarié. L'employeur procède à un contrôle en excluant du contrôle les documents se trouvant dans un dossier marqué comme personnel. Cependant les e-mails en cause ne se trouvent pas dans un tel dossier marqué comme personnel. La Cour d'appel de Versailles estime que ce contrôle est illicite. La Cour de cassation ne partage pas cet avis et estime que « *des courriels et fichiers intégrés dans le disque dur de l'ordinateur mis à disposition du salarié par l'employeur ne sont pas identifiés comme personnels du seul fait qu'ils émanent initialement de la messagerie électronique personnelle du salarié* ».
  - ***CA Luxembourg, 3 mars 2011, n°35462*** : Un salarié reçoit sur son adresse e-mail privée un certain document à intitulé spécifique. Ledit document est ensuite « redécouvert » sur l'ordinateur par l'employeur, alors qu'il y a été effacé. Le salarié estime que l'employeur a violé le secret des correspondances. La Cour rappelle, en se référant la jurisprudence de la Cour européenne des Droits de l'homme, puis à l'arrêt Nikon que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances* ». Cependant elle estime que l'intitulé du document « *ne dénotait a priori aucun caractère privé* » et estime qu'il n'y a pas lieu de faire abstraction du document.

Surveillance des outils informatiques

- Test de **proportionnalité** :
  - un contrôle général de toutes les données tout comme une surveillance permanente des salariés sont à considérer comme disproportionné.
  - ***« progressive Kontrollverdichtung »*** (graduation dans l'intensification de la surveillance)
  - La présence de la personne concernée est exigée pour prendre connaissance du contenu de fichiers marqués comme privés.
- Information spécifique préalable
- Droit d'accès spécifique
- Mesures de sécurité
- Rôle des administrateurs systèmes/réseaux
- Fichiers de journalisation

Systèmes de reconnaissance biométrique

- Notion de **donnée biométrique** :
  - caractéristique physiologique ou comportementale d'un individu traduite en une suite informatique et numérique.
  - exemples : une empreinte digitale, un système et une configuration des veines, la voix
- L'utilisation de données biométriques à des fins d'identification ou d'authentification
  - considéré comme **particulièrement intrusive** dans la vie privée de la personne concernée
  - donnée est obtenue à partir d'un élément du corps humain qui la désigne ou la représente de façon immuable
- Distinction dispositifs biométriques à traces / sans trace :
  - **Dispositif biométrique à traces**
    - traces laissées par les personnes à leur insu sur tous les objets qu'elles touchent. Elles peuvent être capturées et reproduites à l'insu des personnes concernées.
    - ex. empreintes digitales et palmaires
  - **Dispositif biométrique sans traces**
    - ex. contour de la main, réseau veineux des doigts, etc.

Systèmes de reconnaissance biométrique

- Critères de **légitimité** admis :
  - L.261-1(1).1 : sécurité et santé des travailleurs (cas limités, p. ex. accès à un laboratoire avec substances dangereuses, accès à des zones sensibles d'un tribunal où se trouvent des détenus)
  - L.261-1(1).2 : protection des biens (p.ex. accès à des locaux contenant des biens ayant une valeur significative)
  - L.261-1(1).5 : contrôle des horaires de travail (système de pointage au moyen d'un lecteur biométrique)
  - 10 (1).a : exclusivement consentement si surveillance des tiers
- **Nécessité** :
  - système possible que si absolument nécessaire pour les finalités poursuivies
- **Proportionnalité** :
  - au stade actuel des technologies utilisées, la CNPD autorise toujours:
    - Les systèmes contenant des données biométriques qui ne laissent pas de traces, peu importe si les données biométriques sont stockées de façon centralisée ou non.
      - Raisonnement : ces systèmes ne peuvent pas être utilisés à l'insu des personnes concernées.
    - Les traitements de données biométriques qui sont stockées de façon décentralisée sur un support amovible (p. ex. un badge, une carte magnétique), peu importe qu'elles laissent des traces ou non.
  - Par contre, la CNPD n'autorise que dans des hypothèses particulières :
    - Les systèmes contenant des données biométriques qui laissent des traces lorsque les données biométriques ou gabarits sont stockées dans une base de données centralisée.

La protection de la vie privée au travail

Conférence du Jeune Barreau de Luxembourg

CONFÉRENCE DU JEUNE BARREAU DE LUXEMBOURG

Questions?

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Auditoire BGL BNP Paribas

28 février 2014

Gérard Lommel

Président

Commission nationale pour la protection des données

1, avenue du Rock’n’Roll
L-4361 Esch-sur-Alzette (Belval)
261060-1
www.cnpd.lu
info@cnpd.lu