CHAMBRE DES SALARIES
LUXEMBOURG

N° 4 - OCTOBRE 2014

dialogue

THÉMATIQUE

LA SURVEILLANCE SUR LE LIEU DE TRAVAIL
DIE ÜBERWACHUNG AM ARBEITSPLATZ

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

LA SURVEILLANCE SUR LE LIEU DE TRAVAIL

Version française des pages 1 à 52
Französiche Version von Seite 1 bis 52

Version allemande des pages 53 à 108
Deutsche Version von Seite 53 bis 108

Impressum

Éditeurs

Chambre des salariés
18, rue Auguste Lumière
L-1950 Luxembourg
T. (+352) 27 494 200
F. (+352) 27 494 250
www.csl.lu • csl@csl.lu

Jean-Claude Reding, président
Norbert Tremuth, directeur

Commission nationale pour la protection des données
1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette
T. (+352) 26 10 60 -1
F. (+352) 26 10 60 - 29
www.cnpd.public.lu • info@cnpd.lu

Gérard Lommel, président
Thierry Lallemang, membre effectif
Pierre Weimerskirch, membre effectif

Impression
Imprimerie WePrint

Distribution
Librairie « Um Fieldgen Sàrl »
3, rue Glesener
L-1634 Luxembourg
T. (+352) 48 88 93
F. (+352) 40 46 22
info@libuf.lu

ISSN : 5-453002-011003

Préface

Il va sans dire que les nouvelles technologies de l'information et de communication (NTIC) prennent un essor de plus en plus fulgurant et une influence de plus en plus forte dans les relations privées et professionnelles des citoyens.

Si les échanges de données à caractère personnel sont ainsi devenus une réalité et une nécessité pour le développement des activités économiques de notre pays, force est toutefois de constater que ces données envahissent progressivement notre vie privée. Ce développement inquiétant touche tant la sphère privée des individus que leur environnement professionnel.

C'est sur le lieu de travail que s'opposent et doivent donc être mises en balance de façon équilibrée les intérêts des employeurs destinés à assurer la bonne marche et le développement de l'entreprise et ceux des salariés soucieux de protéger leur vie privée. La loi et la jurisprudence ont posé les règles applicables. Le droit des salariés au respect de leur vie privée sur le lieu de travail a été reconnu par la jurisprudence de la Cour européenne des droits de l'homme.

La finalité de la présente publication est d'informer le lecteur sur les droits et obligations des salariés et des employeurs sur le lieu de travail en matière de traitement des données à caractère personnel à des fins de surveillance ainsi que sur le rôle important que joue la Commission nationale pour la protection des données (CNPD) dans cette matière.

Dans un premier temps sont exposés les deux régimes applicables au traitement de données à caractère personnel à des fins de surveillance :

- les traitements à des fins de surveillance des tiers (régime général),
- les traitements à des fins de surveillance des salariés sur le lieu de travail (régime spécifique).

Jean-Claude REDING
Président de la CSL

Gérard LOMMEL
Président de la CNPD

Dans un deuxième temps sont analysées les différentes formes de surveillance qui sont utilisées sur le lieu de travail telles que :

- la vidéosurveillance,
- le contrôle de l'utilisation des outils informatiques,
- l'enregistrement des conversations téléphoniques,
- les systèmes de reconnaissance biométrique,
- les dispositifs de géolocalisation et
- les systèmes de surveillance des accès et des horaires de travail.

Pour chaque forme de surveillance, les auteurs ont essayé de l'illustrer dans la mesure du possible à l'aide de cas jurisprudentiels.

La CSL et la CNPD espèrent que la présente publication réussira à éclairer le lecteur sur les droits et obligations du salarié et de l'employeur en matière de traitement des données à caractère personnel à des fins de surveillance sur le lieu de travail.

Luxembourg, octobre 2014

Sommaire

Sommaire

1

1. Introduction

Le domaine des nouvelles technologies connaît de nos jours un développement fulgurant. L'utilisation de ces nouvelles technologies est à l'origine d'une mutation profonde et inexorable au sein de notre société dans son ensemble. Alors que leurs apports bénéfiques sont incontestables, le constat inévitable est que ces technologies deviennent également de plus en plus envahissantes et intrusives à notre égard. Et ce développement inquiétant touche aussi bien la sphère privée des individus que leur environnement professionnel.

Le milieu du travail n'est pas épargné par les dernières avancées réalisées dans le domaine de la technologie. Dans un contexte où l'employeur cherche à gérer efficacement et à rentabiliser au maximum son entreprise, celui-ci entend aussi mettre à son profit les nouvelles technologies ; or, celles-ci permettent de suivre l'activité des salariés avec un niveau de détail impensable il y a quelques années.

Qu'il s'agisse des derniers développements en matière de géolocalisation, de vidéosurveillance, de biométrie ou de systèmes informatiques permettant une surveillance minutieuse de l'usage des outils informatiques, le contrôle des activités des salariés à l'aide de ces nouvelles technologies s'est extrêmement diversifié au cours des dernières années. Le développement du concept BYOD (*« bring your own device »*) suscite lui aussi la controverse entre les droits et intérêts de l'employeur et le respect de la vie privée des salariés.

Tous ces dispositifs enregistrent évidemment de nombreuses données à caractère personnel relatives aux salariés. Leur utilisation est dès lors susceptible de porter gravement atteinte aux droits des salariés et au respect de leur vie privée sur le lieu de travail, droit qui a été consacré par la jurisprudence européenne : *« 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, Niemietz c. Allemagne, 16 décembre 1992.** Voir en ce même sens : **CEDH, Halford c. Royaume-Uni, 27 juillet 1997 ; CEDH, Copland c. Royaume-Uni, 03 avril 2007 ; CEDH, Peev c. Bulgarie, 26 juillet 2007.**

Pour contrecarrer toute dérive potentielle, le législateur luxembourgeois a mis en place un régime juridique spécifique applicable aux traitements de données à des fins de surveillance, qui traduit en quelque sorte une mise en balance des intérêts divergents qui sont, d'une part pour l'employeur, le droit de veiller au bon fonctionnement de son entreprise, et d'autre part pour les salariés, le droit de bénéficier du respect de leur vie privée sur leur lieu de travail.

Comment concilier ces droits de chacun lors de la mise en place d'une surveillance sur le lieu de travail ? Quelles sont les dispositions légales à respecter ? Quelles peuvent être les raisons amenant un employeur à mettre en œuvre une surveillance ? Quelles mesures doivent-ils adopter pour se conformer à la loi ? De quels droits disposent les salariés ? Comment sont-ils protégés ?

La présente brochure a pour objet d'apporter des réponses à toutes ces questions.

2

2. La notion de surveillance

La loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel (ci-après : « la loi modifiée du 2 août 2002 » ou « la loi ») transpose en droit national la directive européenne 95/46/CE du Parlement européen et du Conseil 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.

Il y a lieu de noter que ladite directive ne contient pas de dispositions spécifiques relatives à la surveillance. Or, soucieux des droits des salariés et des citoyens, le législateur luxembourgeois – alors que la directive ne l'interdit pas – a souhaité régler cette matière dans la loi. Cette dernière définit la « surveillance » de la façon suivante :

« 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. »[1]

Il découle de cette définition légale très large que la notion de surveillance englobe des formes de surveillance extrêmement variées telles que par exemple :

- la vidéosurveillance,
- le contrôle de l'utilisation des outils informatiques (par exemple logs des sites visités sur Internet, vérification des courriers électroniques envoyés et reçus, utilisation faite du réseau interne en entreprise, etc.),
- l'enregistrement des conversations téléphoniques,
- les systèmes de reconnaissance biométrique,
- les dispositifs de géolocalisation,
- les systèmes de surveillance des accès et des horaires de travail.

Avant d'analyser plus en détail ces différents types de surveillance et leurs particularités, il convient en premier lieu d'analyser les dispositions spécifiques relatives à la surveillance pour ensuite passer à une analyse plus approfondie des principes s'appliquant à la surveillance sur le lieu du travail.

1 *Article 2 (p) de la loi modifiée du 2 août 2002.*

3

3. La législation luxembourgeoise

Le législateur, dans un souci de protection des personnes, a mis en place un cadre légal plutôt restrictif concernant la mise en œuvre de traitements de données à des fins de surveillance. Eviter le phénomène de *« big brother is watching you »*, tel fut l'un des objectifs principaux du législateur en mettant en place ce régime spécifique à la surveillance[2], qui se distingue des systèmes implémentés chez nos voisins et qui, pour la plupart, sont moins restrictifs que le système retenu au Luxembourg. Cette approche restrictive a permis de garantir un niveau de sécurité juridique important, tout en minimisant les conflits entre les intérêts en cause.

La loi modifiée du 2 août 2002 énumère de façon limitative les cas dans lesquels une surveillance peut être effectuée et elle distingue clairement entre deux régimes :

- les traitements à des fins de **surveillance des tiers** (Article 10 de la loi) (régime général)
- les traitements à des fins de **surveillance des salariés sur le lieu de travail** (ancien article 11, remplacé par l'article 11 nouveau[3]).

L'article 11 nouveau est applicable aux traitements de données à caractère personnel à des fins de surveillance opérés par l'employeur à l'égard de ses salariés. Il renvoie aux conditions spécifiques énumérées à l'article L.261-1 du Code du Travail. Pour que ce régime s'applique, le critère retenu est celui de l'existence d'un **lien de subordination** juridique entre le responsable du traitement et la personne concernée par la surveillance. En cas de doute sur l'existence du rapport de subordination juridique, il suffit de se référer aux critères dégagés par la jurisprudence nationale en la matière[4]. Notons également que, dans le cadre de l'article 11 nouveau, on assimile au terme *« salarié »* également les fonctionnaires et agents publics, ainsi que les travailleurs intérimaires, mais non pas les salariés de prestataires externes.

Le régime de l'article 10 constitue le régime général applicable à toutes les situations en dehors du contexte de l'emploi. Cet article est donc applicable à tous les cas non couverts par l'article 11 nouveau. Par conséquent, il s'applique aux traitements à des fins de surveillance par un responsable du traitement envers des tiers. Par tiers, on entend toute personne autre que les salariés d'un responsable de traitement donné, c'est-à-dire toute personne étrangère au lien de subordination juridique précité. Ainsi, sont considérés comme tiers sur un lieu du travail par exemple les clients, les visiteurs, les fournisseurs, les consultants externes, etc.

Dépendant du moyen de surveillance utilisé, il se peut qu'un même traitement tombe dans le champ d'application de l'article 10 et de l'article 11, en fonction de la personne concernée (tiers ou salarié). De ce fait, la surveillance de tiers devra également être abordée brièvement dans la présente publication. Les deux régimes s'appliquent très souvent conjointement surtout en matière de vidéosurveillance dans la mesure où des personnes non salariées, à l'égard du responsable du traitement, sont également concernées par la surveillance. Tel est par exemple le cas d'une caméra dans une grande surface qui filme aussi bien les salariés du magasin (article 11 nouveau) que des tiers (clients, article 10). Dans le même ordre d'idées, l'enregistrement des conversations téléphoniques par une banque peut concerner aussi bien les employés (article 11 nouveau) que les clients (article 10).

2 *V. doc. parl. 4735/00, p. 36.*

3 *V. art. 10 de la loi du 27 juillet 2007 portant modification de la loi du 2 août 2002.*

4 *« 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 », v.* ***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****, cités dans : 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.*

4. Quels peuvent être les objectifs poursuivis par l'employeur ? La finalité, le concept-clé dans tout traitement de données

Tout traitement de données poursuit par nature un certain but ; fixer clairement et précisément cet objectif permet non seulement de déterminer concrètement les opérations à effectuer pour l'atteindre, mais également d'en circonscrire ses limites exactes[5].

La détermination de la ou des finalité(s) à atteindre est un prérequis nécessaire afin de pouvoir appliquer et apprécier les autres critères qui y sont indissociablement attachés. Ces critères comprennent le caractère déterminé, explicite et légitime de cette finalité, ainsi que celui du traitement ultérieur incompatible avec cette finalité[6]. Le principe de la délimitation de la finalité **détermine donc le périmètre** dans lequel des données personnelles peuvent être collectées, traitées et utilisées ou non ultérieurement. Ce principe-clé permet de protéger la personne concernée en limitant la manière de laquelle un responsable du traitement peut utiliser les données et contribue donc à augmenter aussi bien la transparence, la sécurité juridique et la prévisibilité d'un traitement de données à caractère personnel.

Le **responsable du traitement** est *« 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 »*[7].

Par **finalité déterminée**, on comprend donc une finalité définie de manière tellement précise qu'elle permet une délimitation claire et non pas vague du domaine d'application du traitement.

Pour être considérée comme **explicite**, la finalité doit être exprimée de manière suffisamment claire et sans ambiguïté (pas de finalité cachée).

La **légitimité** exige que le responsable du traitement ne puisse se baser que sur les critères de légitimité fixés limitativement par la loi. Cependant, dans le cadre d'une surveillance, les conditions de légitimité générales posées à l'article 5 de la loi n'ont pas vocation à s'appliquer. En effet, les articles 10 (surveillance des tiers) et 11 nouveau (surveillance sur le lieu de travail) dérogent aux conditions de légitimité générales posées par l'article 5 de la loi. Par conséquent, les cas d'ouverture, c'est-à-dire les seuls buts reconnus pour lesquels on peut effectuer une surveillance, sont ceux repris par ces deux articles[8]. Une analyse détaillée de ces cas d'ouverture, qui varient en fonction du type de surveillance, est présentée aux points 5.1. et suivants de la présente brochure.

La détermination précise de la finalité est aussi cruciale pour éviter que celle-ci ne soit pas détournée. Un exemple d'un tel détournement de finalité serait l'utilisation d'images provenant d'un système de vidéosurveillance, installé aux fins de protéger l'accès au bâtiment du responsable du traitement, mais utilisées par l'employeur pour vérifier les temps de présence de ses salariés. Constitue également un détournement de finalité un système de vidéosurveillance relatif à une chaîne de production visant uniquement les machines, mais dont les images sont utilisées pour surveiller par exemple le comportement ou la performance d'un ou de plusieurs employés.

Il découle de ce qui précède que les finalités pour lesquelles un responsable du traitement peut être amené à surveiller ses salariés varient en fonction du type de surveillance mis en œuvre. Dans un souci de protection des personnes concernées par des mesures

5 *V. doc. parl. 4735/00, p. 30 et s.*

6 *Article 4, paragraphe (1), lettre (a) de la loi.*

7 *Article 2, lettre (n) de la loi.*

8 *Position confirmée en jurisprudence, v. notamment* ***Trib. Admin. Lux., 15 décembre 2004, n°17890,*** *confirmé par* ***Cour Admin Lux., 12 juillet 2005, n°19234 C ;*** *v. aussi* ***Trib. Admin. Lux., 9 mai 2005, n°18680 ; Trib. Admin. Lux., 21 mai 2007, n°22050****.*

4

4. Quels peuvent être les objectifs poursuivis par l'employeur ? La finalité, le concept-clé dans tout traitement de données.

de surveillance lesquelles présentent un risque particulier au regard de la vie privée des salariés, le législateur a opté pour un régime d'autorisation préalable. À cet égard, la Commission nationale pour la protection des données (ci-après « la Commission nationale » ou « la CNPD ») dispose d'un pouvoir d'appréciation dans l'analyse de la **nécessité** et de la **proportionnalité**[9] des mesures de surveillance envisagées par l'employeur avant de lui accorder une autorisation.

Par exemple, une surveillance au moyen d'un système de géolocalisation des voitures d'une entreprise peut être considérée comme nécessaire et proportionnelle, alors que le salarié est seulement surveillé de manière indirecte par le biais du véhicule. Cependant, si le dispositif de géolocalisation est porté sur le corps du salarié, la Commission nationale estime, sauf hypothèse très exceptionnelle, que le moyen de surveillance est disproportionné, car il permet à l'employeur de surveiller le déplacement du salarié lui-même à la seconde et au mètre près.

La détermination des finalités d'un traitement par l'employeur constitue donc clairement un facteur déterminant pour savoir si une autorisation lui sera accordée ou non.

9 *Confirmé en jurisprudence, v. notamment* ***Trib. Admin. Lux., 15 décembre 2004, n°17890****, confirmé par* ***Cour Admin. Lux., 12 juillet 2005, n°19234 C*** *; v. aussi* ***Trib. Admin.Lux., 21 mai 2007, n°22050****.*

5. Comment sont protégés les salariés ?

La loi modifiée du 2 août 2002 assure une protection renforcée aux salariés et aux tiers (personnes non salariées) concernés par une mesure de surveillance. Cette protection est notamment garantie par :

- un catalogue restreint et détaillé des cas d'ouverture permettant une surveillance (**Chapitre 5.1.**) ;
- l'examen préalable par la CNPD au cas par cas et dont l'autorisation tient compte, d'un côté, du droit des salariés au respect de leur vie privée sur le lieu de travail et, de l'autre côté, de l'intérêt légitime de l'employeur à mettre en place un système de surveillance (analyse de la nécessité et proportionnalité des mesures de surveillance envisagées / balance des intérêts en cause) (**Chapitre 5.2.**) ;
- le respect d'un certain nombre d'obligations par le responsable du traitement (**Chapitre 5.3.**).

5.1. Les cas dans lesquels la surveillance est possible sont limités par la loi

5.1.1. Surveillance par l'employeur sur le lieu du travail

L'article 11 nouveau (qui renvoie à l'article L.261-1 du Code du Travail) permet à l'employeur de surveiller sous certaines conditions ses salariés sur le lieu du travail. Les cas d'ouverture permettant une telle surveillance ont été limitativement énumérés par le législateur, c'est-à-dire il faut obligatoirement légitimer un traitement en se basant sur une ou plusieurs des cinq conditions de légitimité retenues par la loi ; aucune autre (non listée) ne pourra être acceptée. En effet, la Commission nationale estime qu'il convient d'adopter une lecture littérale et une interprétation restrictive de cette disposition légale, car le législateur a édicté une liste fermée de conditions de légitimité expresses auxquelles il entendait restreindre les cas de surveillance licites.

L'article L.261-1 du Code du Travail dispose qu'*« un traitement n'est possible que s'il est nécessaire* :

1. *pour les besoins de sécurité et de santé des travailleurs, 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 travailleur, lorsqu'une telle mesure est le seul moyen pour déterminer la rémunération exacte, ou*
5. *dans le cadre d'une organisation de travail selon l'horaire mobile conformément au Code du Travail. »*

Le premier point de l'article L.261-1 peut être invoqué par un employeur lorsque, en fonction des circonstances, l'activité de ses salariés est de nature à porter potentiellement atteinte à leur sécurité ou leur santé (ce qui peut impliquer notamment une atteinte à leur intégrité physique), soit parce que les fonctions qu'ils exercent sont périlleuses (machines dangereuses, présence de substances toxiques), soit parce que les salariés pourraient faire l'objet d'attaques physiques.

Tel est par exemple le cas d'une société de transport de fonds et de valeurs ayant recours à un système de géolocalisation. En raison de la valeur des biens qu'ils ont sous leur garde, les salariés d'une telle société peuvent potentiellement faire l'objet d'attaques phy-

5

5. Comment sont protégés les salariés ?

siques – la mesure de surveillance par géolocalisation serait donc à considérer comme légitime si le responsable du traitement se base sur ce cas d'ouverture. Un autre exemple est la vidéosurveillance dans une station d'essence, une bijouterie ou une banque. Une telle mesure de surveillance peut contribuer à prévenir des atteintes à l'intégrité physique des employés dans l'hypothèse d'un braquage, d'un hold-up voire même d'une prise d'otages.

Le deuxième point de l'article L.261-1 peut être invoqué pour légitimer une surveillance visant à prévenir des actes de vol ou de vandalisme. La **notion de protection des biens** englobe les biens corporels (c'est-à-dire les biens meubles et immeubles) mais aussi les biens incorporels (droits de propriété intellectuelle, secrets d'affaire, portefeuilles de créances, etc.). Mais, la CNPD estime que la notion ne doit pas comprendre la protection d'intérêts économiques de l'entreprise autres que ceux liés à des biens corporels clairement identifiables. Invoquer un risque de préjudice financier, un coût injustifié ou un manque à gagner est insuffisant comme justification.

Ce critère de légitimation de l'article L.261-1 peut par exemple être invoqué par un commerçant qui envisage de surveiller son stock de marchandises contre le vol.

Le troisième cas de figure de l'article L.261-1, moins commun que les deux premiers, vise la seule surveillance incidente des salariés au cours de la surveillance principale d'un système de production mécanisé tel que par exemple une chaîne automatisée d'assemblage de circuits électroniques. La surveillance vise donc principalement les machines et ce n'est que de manière accessoire et fortuite que les salariés sont susceptibles d'être surveillés. Dans le cadre d'une vidéosurveillance, un exemple serait celui d'un technicien qui doit intervenir sur une machine de la chaîne de production pour la réparer et qui pendant ce temps est filmé par des caméras. Le but principal de ces caméras n'est pas de surveiller le technicien, mais bien de déceler par exemple un défaut dans la production ou un arrêt sur les chaînes de production. Dans ce cas, la surveillance des salariés est accessoire, le but principal recherché par la surveillance est le contrôle de l'infrastructure matérielle, des machines et des outils que l'employeur possède dans le cadre de son activité professionnelle.

Le quatrième point est très rare, voire inapplicable en pratique. L'inapplicabilité de ce cas de figure résulte des trois conditions cumulatives qui ont été posées par le législateur, à savoir : (i) il faut qu'il s'agisse d'un contrôle temporaire, donc la surveillance doit être strictement limitée dans le temps ; (ii) le contrôle ne peut que porter sur la production ou les prestations du salarié ; et (iii) cette mesure doit être le seul moyen pour déterminer le salaire exact. Pour une illustration, il est renvoyé vers le point 7.1.2.1.

Le cinquième point peut être invoqué par un employeur voulant contrôler les horaires de travail et les temps de présence de ses salariés sur le lieu de travail.

5.1.1.1. Rôle spécifique du comité mixte d'entreprise

Dans les cas visés aux points 1, 4 et 5 de l'article L.261-1 du Code du Travail, le comité mixte d'entreprise, s'il est institué, a un **pouvoir de décision** tel que défini à l'article L.423-1, points 1 et 2 du Code du Travail. Selon les documents parlementaires, *« la finalité première de l'intervention du comité mixte doit être d'assurer que les principes de proportionnalité et de fonctionnalité soient en tout état de cause respectés dans la mise en œuvre de la procédure de surveillance*[10]*»*.

Dans ces trois cas de figure, l'accord du comité mixte doit donc être obtenu préalablement à l'introduction de la demande d'autorisation et doit être joint au dossier de la demande formulée auprès de la CNPD. La décision du comité mixte constitue ainsi en quelque sorte un premier filtre dans l'appréciation de la mise en œuvre de la surveillance. Les finalités des deux

10 Doc. parl. n°4735/07, p. 4.

autres cas d'ouverture (protection des biens et contrôle du processus de production portant sur les machines) *« ne rentrent pas dans le domaine de compétence du comité mixte d'entreprise* [11] *»* et *« … relèvent de la responsabilité de l'employeur qui doit garder le pouvoir de décision sur l'organisation de l'entreprise*[12] *»*.

Si l'entreprise en question n'a pas institué de comité mixte, un accord de la délégation du personnel n'est pas obligatoire ou nécessaire. Cependant, l'employeur est en tout état de cause obligé d'informer les instances de la représentation du personnel de la mise en œuvre d'un traitement à des fins de surveillance[13] (voir aussi le point 5.3.1.).

Notons cependant que la portée du pouvoir décisionnel du comité mixte a été relativisée par une jurisprudence de la **Cour d'Appel du 26 janvier 2006**[14], qui retient que, dans cette espèce, la non-saisine du comité mixte n'est pas susceptible d'influer sur le sort du litige, alors même que *« la délégation du personnel avait constaté que le système présentait des lacunes »*.

5.1.1.2. Exclusion du consentement des salariés comme critère de légitimation

La loi prévoit expressément que le consentement du salarié est exclu comme hypothèse de légitimation de la surveillance sur le lieu de travail. L'employeur ne peut donc pas demander à ses salariés de signer un document de consentement qui rendrait ainsi légitime les mesures de surveillance envisagées par l'employeur.

Cette exclusion de la loi est nécessaire afin de protéger l'employé qui se trouve dans une situation d'infériorité par rapport à son patron[15]. Ce dernier, s'il pouvait faire légalement usage du consentement de son employé, pourrait par exemple l'insérer systématiquement dans le contrat de travail et ainsi imposer l'accord automatique du salarié à des mesures de surveillance. Le principe du respect de la vie privée du salarié au travail s'en trouverait considérablement affaibli, voire invalidé.

5.1.2. Surveillance des personnes non salariées (« tiers »)

Dans le chapitre sur la législation luxembourgeoise (point 3, page 6), on a vu qu'il est possible qu'un même traitement tombe dans le champ d'application de l'article 10 et de l'article 11, en fonction de la personne concernée (tiers ou salarié). Selon les conditions de l'espèce, ces deux régimes peuvent donc s'appliquer conjointement. Le cas le plus fréquemment rencontré concerne le domaine de la vidéosurveillance où des personnes non salariées à l'égard du responsable du traitement sont également touchées par les mesures de surveillance. Il convient dès lors de fournir quelques explications élémentaires relatives à l'application du régime général de l'article 10.

Les conditions pour pouvoir surveiller des personnes non salariées sont énumérées à l'article 10 de la loi modifiée du 2 août 2002. Dans ces cas, la surveillance se fait en dehors de tout lien de subordination juridique[16] entre le responsable du traitement et la personne concernée par la surveillance.

Cet article dispose que *« le traitement à des fins de surveillance ne peut être effectué que :*

(a) *si la personne concernée a donné son consentement, ou*

11 *Doc. parl. n°4735/13, p. 21.*

12 *Ibid.*

13 *Art. L.261-1, para. (2) du Code du Travail.*

14 ***Cour Appel Lux, 26 janvier 2010, n°29384.***

15 *V. supra. les développements par rapport au lien de subordination juridique.*

16 *V. supra., note de bas de page n°4 au point 3., p. 10.*

5

5. Comment sont protégés les salariés ?

(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 nécessaire 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. »*

Le premier cas d'ouverture prévoit que le responsable du traitement peut obtenir le consentement de la personne concernée (« non-salariée ») pour légitimer la mesure de surveillance. Par **consentement**, il faut comprendre *« toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée ou son représentant légal, judiciaire ou statutaire accepte que les données à caractère personnel fassent l'objet d'un traitement*[17] *».*

La loi n'exige pas un écrit, mais il est néanmoins recommandé, afin que le responsable du traitement soit en mesure d'en rapporter la preuve concrète en cas de besoin. Le consentement n'est toutefois pas adapté ou approprié pour être invoqué en toute circonstance. Le meilleur exemple est probablement l'impossibilité de demander le consentement à tout tiers soumis à une mesure de vidéosurveillance, c'est-à-dire à toute personne susceptible de traverser le champ de vision d'une caméra. En pratique, le consentement ne peut trouver application que dans certains cas de figure.

Relevons encore que même si un responsable du traitement peut invoquer comme critère de légitimation le consentement, la CNPD peut toujours être amenée à refuser une surveillance pour des raisons de proportionnalité. Tel peut être le cas par exemple pour certains types de traitements de données biométriques.

Il faut dire que le point (b) a été rédigé dans une optique de surveillance au moyen de caméras vidéo et concerne les lieux (autres que des locaux d'habitation) qui en raison de leurs caractéristiques particulières rendent la surveillance nécessaire pour la sécurité des usagers ou pour la protection des biens. Le point (b) est donc **peu adapté à d'autres types de surveillance**.

La notion de *« lieu d'accès »* à l'article 10 (1) (c) n'a pas été définie dans la loi. Selon l'interprétation de la CNPD, le lieu d'accès doit être compris comme *« l'endroit par lequel on accède à un lieu privé indépendamment de la question de savoir si ce lieu est accessible ou non au public »*. Ce point (c) permet notamment de légitimer un traitement à des fins de surveillance des tiers lorsqu'ils accèdent aux locaux d'un bâtiment, peu importe qu'il s'agisse d'accès extérieurs ou intérieurs. Il peut s'agir par exemple des clients d'un magasin qui sont filmés lorsqu'ils franchissent la porte d'entrée.

Le dernier cas d'ouverture (point (d)) est très rare en pratique. Il peut s'appliquer par exemple à une personne qui se trouve dans une salle de réveil après une opération et dont l'état de santé critique nécessite une surveillance par caméras permanente permettant au personnel médical de réagir immédiatement lorsqu'il y a des complications.

17 *Article 2, lettre (c) de la loi modifiée du 2 août 2002.*

5.2. Exigence d'une autorisation préalable de la CNPD

L'exigence d'autorisation préalable traduit la volonté expresse du législateur luxembourgeois de protéger les personnes physiques de certains traitements *« susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées*[18]*... »*. Parmi ceux-ci figurent notamment les traitements en matière de surveillance sur le lieu de travail étant donné que ceux-ci présentent un risque particulier au regard de la vie privée des salariés sur leur lieu de travail.

Tout responsable du traitement qui envisage de mettre en œuvre un traitement à des fins de surveillance doit solliciter une autorisation préalable auprès de la CNPD. L'unique exception à ce principe concerne l'hypothèse d'une surveillance qui vise exclusivement des tiers, c'est-à-dire une surveillance qui n'est pas effectuée sur un lieu de travail et dont les données ne font pas l'objet d'un enregistrement[19]. Cette condition est à interpréter de manière restrictive, c'est-à-dire dès qu'un salarié du responsable du traitement serait concerné par la surveillance, l'exception ne jouerait pas et une autorisation préalable serait néanmoins nécessaire. Cette exception est cependant très rare en pratique. L'introduction d'une notification préalable auprès de la CNPD reste néanmoins nécessaire pour ce genre de traitement.

Notons encore le régime spécifique de l'article 17 de la loi qui soumet certains traitements non pas à l'autorisation par la CNPD, mais à **l'autorisation par voie de règlement grand-ducal**.

Il s'agit des traitements de données suivants :

- les traitements d'ordre général de la Police grand-ducale et de l'Administration des Douanes et Accises effectués dans le cadre de la prévention, recherche et constatations d'infractions pénales ;
- les systèmes de vidéosurveillance opérés par la Police grand-ducale dans des zones de sécurité situées sur la voie publique ;
- les traitements de l'Armée ;
- les traitements du Service de Renseignements de l'État.

Le contrôle et la surveillance de tous ces traitements ne relève pas de la compétence de la CNPD, mais de celle d'une autorité de contrôle spécifique qui est composée du Procureur Général d'État et de deux membres de la CNPD (pour plus de détail, voir article 17 de la loi).

Relevons enfin que la **loi sur la protection des données ne s'applique pas** aux traitements de données mis en œuvre par une personne physique dans le cadre exclusif de ses activités personnelles ou domestiques[20].

La loi ne s'applique donc pas lorsqu'une personne installe par exemple des caméras vidéo à son domicile, mais celles-ci ne doivent en aucun cas filmer la voie publique ni une propriété avoisinante.

Dans tous les autres cas de figure, dans le cadre de sa compétence d'autorisation, il revient à la Commission nationale de vérifier notamment :

- que les données sont collectées pour des **finalités** déterminées, explicites et légitimes, et ne sont pas traitées ultérieurement de manière incompatible avec ces finalités ;
- que le motif invoqué pour recourir à la surveil-

18 *Doc. parl. n°4735/13, p. 29.*

19 *Art. 14, para. (1), lettre (b) de la loi.*

20 *Art. 3, para. (3) de la loi.*

5

5. Comment sont protégés les salariés ?

lance correspond bien à un critère de **légitimation** prévu par la loi ;

- que la mesure envisagée est bien **nécessaire** et non pas seulement utile ou opportune compte tenu des circonstances concrètes (notamment que les risques que la surveillance vise à prévenir ou à combattre sont suffisamment effectifs et substantiels). En ce sens, la jurisprudence luxembourgeoise a précisé qu'une simple considération d'opportunité ne suffisait pas[21]. Cette jurisprudence fut confirmée en instance d'appel[22] ;
- que l'impact de la surveillance sur les libertés et droits fondamentaux, en particulier la vie privée des personnes touchées, reste supportable et ne soit pas excessif (**proportionnalité**) par rapport à la finalité poursuivie et qu'il n'y ait pas de moyens alternatifs permettant d'aboutir au résultat recherché de façon moins intrusive pour la vie privée des personnes exposées à la surveillance ;
- que les données soient traitées de façon **sécurisée** et soient **conservées** seulement aussi longtemps qu'effectivement nécessaire.

Les décisions de la CNPD visent à établir un juste équilibre entre les différents intérêts en jeu. Elle procède, au moyen d'une analyse détaillée au cas par cas, à une mise en balance des intérêts des personnes concernées, à savoir leur droit au respect de leur vie privée ainsi que de l'intérêt légitime que peut avoir un employeur à mettre en œuvre un traitement à des fins de surveillance.

La jurisprudence a clairement établi que la CNPD dispose d'un pouvoir d'appréciation *in concreto* dans l'analyse qu'elle doit effectuer pour autoriser des traitements de données. Dans un jugement du Tribunal administratif de 2004, il a été jugé que c'était bien le rôle de la CNPD de trancher au cas par cas. L'argument selon lequel la CNPD devrait se limiter uniquement à l'application formelle de la loi au lieu de faire une appréciation, a été réfuté par le tribunal, comme suit : « *... le reproche adressé à la Commission d'avoir apprécié en l'espèce l'opportunité de la mise en place du système de vidéosurveillance préconisé et d'avoir ainsi excédé ses pouvoirs, laisse d'être fondé, la CNPD ayant au contraire suivi l'approche prétracée par le législateur en appréciant le caractère nécessaire ou non du dispositif envisagé par rapport au besoin de sécurité et de santé des travailleurs ainsi que par rapport au besoin de protection des biens de l'entreprise* ».[23]

Cette position retenue par le Tribunal administratif a été confirmée en appel[24] : « *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*

21 ***Trib. Admin. Lux., 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 ».*

22 ***Cour Adm. Lux., 12 juillet 2005, n°19234C, p. 11 et s.****, « La CNPD a en l'espèce procédé à juste titre à l'évaluation de la nécessité du traitement faisant l'objet de la demande de la société X par rapport aux différents cas d'ouverture limitativement énoncés par la loi à cet égard, puisqu'elle a reçu par le législateur la mission consistant précisément à vérifier si la demande soumise à autorisation préalable rentre dans les prévisions des dispositions de la loi. Il ne suffit partant pas que la demanderesse en autorisation, en l'espèce l'appelante, affirme avoir l'intention de protéger ses biens au moyen du système de vidéosurveillance envisagé par elle, mais elle doit au contraire rapporter la preuve de la pertinence de ses affirmations. C'est partant à bon droit que la CNPD a pu procéder à l'analyse de la nécessité invoquée par l'appelante et il y a lieu de confirmer les conclusions retenues à cet égard par les premiers juges ».*

23 ***Trib. Admin. Lux, 15 décembre 2004, n°17890.***

24 ***Cour Admin. Lux., 12 juillet 2005, n°19234C.***

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 autorisations de la CNPD sont dans la plupart des cas assorties de conditions et/ou de recommandations. Celles-ci seront analysées de plus près dans le contexte des différents types de surveillance présentés au point 7. qui suit.

5.3. Obligations légales à respecter par l'employeur

À part l'obligation de respecter les principes de finalité, de légitimité, de nécessité et de proportionnalité, le responsable du traitement doit encore être attentif à un certain nombre d'exigences de fond et de forme avant de pouvoir mettre en œuvre un traitement à des fins de surveillance.

La loi modifiée du 2 août 2002 sur la protection des données retient certaines exigences auxquelles doit satisfaire tout traitement de données. Le responsable du traitement devra en effet veiller à respecter son *devoir d'informer* les personnes concernées qu'un traitement de leurs données a lieu. Il devra également assurer un *droit d'accès, de suppression* et de *modification* de leurs données et les *conserver* de *façon limitée* dans le temps tout en garantissant leur *confidentialité* et leur *sécurité*.

N.B. : Nous voudrions souligner que toutes les obligations légales analysées ci-après s'appliquent bien évidemment à tous les types de surveillance développés plus loin à la section 7. En effet, nous n'entendons pas revenir en détail à toutes ces obligations aux points 7.1. à 7.6.

5.3.1. Obligation d'informer les salariés et la représentation du personnel - le principe de transparence

Information des salariés

Tout responsable du traitement est obligé d'informer de manière claire et non équivoque les personnes concernées du traitement qu'il met en œuvre. Tout salarié a donc le droit[25] de savoir si ses données à caractère personnel sont traitées et pour quelles finalités. Les salariés doivent obligatoirement être informés lors de la collecte, ou au plus tard lors de l'enregistrement des données les concernant.

Le droit à l'information connaît cependant plusieurs exceptions[26], notamment lorsque le traitement est nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la constatation et la poursuite d'infractions pénales, etc. En pratique, ces exceptions peuvent rarement être invoquées par un employeur en ce qui concerne un traitement à des fins de surveillance.

Le principe de transparence implique également que des mesures de surveillance **cachées** ne peuvent jamais être mises en œuvre par un responsable du traitement, ni autorisées par la CNPD. En droit national, seul un juge d'instruction peut ordonner des mesures de surveillance cachées (art. 88-1 et 88-2 CIC).

Information de la représentation du personnel

Il ne suffit pas que l'employeur informe uniquement les salariés exposés à la surveillance. La loi prévoit en plus que le comité mixte, ou à défaut la délégation du personnel, ou à défaut encore, l'Inspection du Travail

25 *Art. 26 de la loi modifiée du 2 août 2002.*

26 *Art. 27 de la loi modifiée du 2 août 2002.*

5

5. Comment sont protégés les salariés ?

et des Mines soient spécialement informés de la mise en œuvre de la surveillance. Il s'agit d'une obligation d'information renforcée, applicable dans le cadre d'une surveillance sur le lieu de travail[27].

Information des tiers

Lorsque des tiers (non-salariés) sont également concernés par la surveillance, il est évident que ceux-ci doivent aussi être informés conformément à l'article 26 de la loi.

5.3.2. Respect du droit d'accès et de rectification

Le salarié peut demander à son employeur d'obtenir sans frais, à des intervalles raisonnables et sans délais excessifs, la communication, sous une forme intelligible, de ses données faisant l'objet d'un traitement, ainsi que de toute information disponible sur l'origine des données. Il a également le droit de faire rectifier ou supprimer des informations erronées ou obsolètes[28].

Comme pour le droit à l'information, la loi prévoit ici aussi certaines exceptions[29] au droit d'accès de la personne concernée. En pratique, ces exceptions peuvent rarement être invoquées par un employeur en ce qui concerne un traitement à des fins de surveillance.

5.3.3. Durée de conservation limitée

Les données traitées ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une **durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées et traitées**[30].

Le stockage ou l'enregistrement des données doit donc être limité dans le temps. La finalité du traitement de données sert comme vecteur pour déterminer la période de conservation appropriée. Après écoulement du délai de conservation retenu, les données doivent en principe être détruites. En matière de vidéosurveillance, par exemple, la CNPD autorise en principe un délai de conservation des images de 8 jours. Dans des cas spécifiques, ce délai peut éventuellement être augmenté jusqu'à une période maximale de 30 jours.

Il est évident que les données ne doivent pas être détruites après l'écoulement de ce délai lorsqu'elles font l'objet d'une transmission aux autorités publiques et judiciaires compétentes pour constater ou pour poursuivre une telle infraction pénale[31] (par exemple les images sur lesquelles est constaté un vol à l'étalage).

La conservation illimitée de données anonymisées ou rendues anonymes est possible. L'anonymisation doit cependant être interprétée de manière restrictive, une pseudonymisation ou une codification n'étant pas suffisantes. L'anonymisation doit être **irréversible**, c'est-à-dire effectuée de manière à ne plus jamais permettre une ré-identification de la personne à laquelle se rapportent les données, peu importe les moyens mis en œuvre.

27 Art. L.261-1, para. (2) du Code du Travail.

28 Art. 28 de la loi modifiée du 2 août 2002.

29 Art. 29 de la loi modifiée du 2 août 2002.

30 Conformément à l'article 4 paragraphe (1) lettre (d) de la loi modifiée du 2 août 2002.

31 V. article 10 paragraphe (3) lettres (b) et (c) de la loi modifiée du 2 août 2002.

5.3.4. Adoption de mesures de sécurité et de confidentialité adéquates

Des mesures de sécurité organisationnelles et techniques suffisantes doivent être mises en place[32], afin d'assurer la protection des données traitées contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute forme de traitement illicite.

Le responsable du traitement doit également assurer que ses subordonnés (salariés ou autres) traitent les données dans le respect des conditions de la loi modifiée du 2 août 2002.

S'il a recours à un sous-traitant, il doit s'assurer que son prestataire (sous-traitant) remplisse également les conditions de sécurité des données imposées par la loi. Le responsable du traitement, malgré le fait d'avoir recours à un tel sous-traitant, reste néanmoins toujours responsable de l'usage fait de ces données.

Notons encore que les mesures de sécurité peuvent varier en fonction de la nature de la surveillance et de l'état de l'art et des coûts liés à leur mise en œuvre.

32 Conformément aux articles 22 et 23 de la loi modifiée du 2 août 2002.

6

6. Quelles sont les sanctions en cas de non-respect de la loi ?

La CNPD ne dispose pas (dans le domaine qui nous occupe) d'un pouvoir de sanction pécuniaire. Ce pouvoir existe seulement dans le cadre de l'application de la loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

Elle dispose cependant du pouvoir de prononcer certaines sanctions administratives à l'encontre du responsable du traitement[33].

Or, il faut souligner que presque la moitié des dispositions de la loi (19 sur 45 articles) sur la protection des données prévoient des sanctions pénales en cas de violation. Ainsi, la mise en œuvre ou l'utilisation d'un système de surveillance qui ne respecte pas les dispositions de la loi, voire les conditions posées par la CNPD peut être constitutive de la commission d'un délit pénal. Un responsable du traitement peut ainsi se voir condamné par un tribunal à une peine d'emprisonnement pouvant aller de huit jours à un an et d'une amende de 251 à 125.000 euros ou d'une de ces peines seulement.

33 Article 33 de la loi modifiée du 2 août 2002.

7. Types de surveillance

Après avoir analysé les conditions et exigences auxquelles sont soumis les traitements de données à des fins de surveillance, les développements qui suivent s'attachent à dresser un panorama des types de surveillance les plus utilisés par les employeurs.

En termes de pourcentage des types de surveillances autorisées par la CNPD, les chiffres se présentent comme suit (moyenne statistique sur une période de 10 ans) :

- Vidéosurveillance : 70 %
- Surveillance de l'usage des outils informatiques : 7%
- Enregistrement des conversations téléphoniques : 8,5%
- Systèmes biométriques : 1%
- Dispositifs de géolocalisation : 5%
- Surveillance des accès aux locaux : 5%
- Contrôle des horaires de travail : 3,5%

7.1. Vidéosurveillance

Les environnements de travail sont de plus en plus équipés de dispositifs de vidéosurveillance. S'ils peuvent être considérés comme légitimes pour assurer la sécurité des salariés ou protéger les biens de l'entreprise, de tels dispositifs constituent en même temps une intrusion dans la vie privée des personnes et touchent à la liberté de pouvoir circuler sans être observé.

7.1.1. Quels peuvent être les objectifs poursuivis par l'employeur ?

Nombreuses sont les raisons pour lesquelles un employeur souhaite installer un dispositif de vidéosurveillance :

- protéger les biens de son entreprise (par exemple marchandises, argent, installations, machines, bâtiments, documents confidentiels, etc.) ;
- veiller à la sécurité du personnel, des clients ;
- identifier les auteurs de vols et d'agressions ;
- sécuriser les accès au site ou aux immeubles ;
- détecter et identifier des comportements suspects ou dangereux susceptibles de provoquer des accidents ou incidents ;
- repérer l'origine d'un incident ;
- alerter les services de secours, d'incendie ou les forces de l'ordre ;
- permettre une évacuation rapide en cas d'incident.

Cette liste n'est qu'exemplative car il peut exister bon nombre d'autres raisons justifiant le recours à un système de vidéosurveillance.

Pour être acceptées, ces raisons ou finalités doivent correspondre au moins à un des cas d'ouverture prévus par la loi (cf. point 7.1.2. ci-après). De plus, il revient à la CNPD d'analyser la nécessité et la proportionnalité des mesures de surveillance envisagées par l'employeur avant de lui délivrer une autorisation (point 7.1.3.).

7.1.2. Dans quels cas la vidéosurveillance est-elle possible ?

7.1.2.1. Vidéosurveillance des salariés

Au moins une condition de légitimité de l'article L.261-1(1) du Code de Travail doit pouvoir être invo-

7

7. Types de surveillance

quée[34] et justifiée par l'employeur. Rappelons que la surveillance des salariés sur le lieu du travail n'est possible que si elle est nécessaire :

- pour les besoins de sécurité et santé des salariés,
- pour les besoins de protection des biens de l'entreprise,
- pour le contrôle du processus de production portant uniquement sur les machines,
- 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
- pour les traitements dans le cadre d'une organisation de travail selon l'horaire mobile conformément au Code du Travail.

Sécurité et santé des salariés

Dans le cadre de ce cas d'ouverture, le responsable du traitement doit justifier de situations ou d'éléments concrets présents dans son entreprise l'amenant à considérer que la sécurité et/ou la santé de ses salariés (employés, stagiaires, intérimaires, apprentis) sont susceptibles d'être mis en danger et que le système de vidéosurveillance aidera à prévenir ce danger. Citons à titre d'exemple, la présence de machines dangereuses, de substances toxiques ou nocives, mais également des fonctions dangereuses comme les transporteurs de fonds et de valeurs, les salariés de banques occupés à la caisse, etc.

L'exemple type est celui des salariés employés dans une station-service. Ce lieu de travail, accessible au public, présente un risque élevé de vols à main armée comme en témoignent les statistiques sur la criminalité. De plus, il existe un risque d'explosion ou d'incendie dû au stockage et à la manipulation d'importantes quantités de produits facilement inflammables et dangereux (hydrocarbures ou autres). Un système de vidéosurveillance peut contribuer à prévenir de tels accidents, mais également à dissuader des hold-up et ainsi des atteintes à l'intégrité physique des salariés.

Protection des biens de l'entreprise

Ce critère de légitimation vise avant tout les surveillances ayant pour but de prévenir des atteintes aux biens corporels, c'est-à-dire des vols ou des actes de vandalisme. En ce qui concerne l'interprétation de la CNPD de la notion de *« protection des biens »*, il est renvoyé au point 5.1.1.

Sont surtout visés ici les vols par les salariés dans les caisses, stocks, etc.

Contrôle du processus de production portant uniquement sur les machines

Ce troisième cas d'ouverture vise la seule surveillance incidente des salariés au cours de la surveillance principale d'un système de production mécanisé et/ou automatisé, telle que par exemple une chaîne automatisée d'assemblage de parts automobiles ou un système de remplissage automatisé de bouteilles dans le cadre d'une manufacture de boissons. Ainsi, la vidéosurveillance ne peut être admise sur base de cette condition de légitimité que si elle permet de déceler un éventuel défaut dans la production et/ou arrêt sur les chaînes de fabrication, permettant ainsi de contrôler le processus de production. La vidéosurveillance doit donc être configurée principalement pour surveiller les machines et ce n'est que de manière incidente et fortuite que les salariés sont susceptibles de traverser le champ de vision des caméras, par exemple lorsqu'ils en vérifient le fonctionnement ou font des travaux de réparation.

Les deux autres cas d'ouverture prévus par la loi ne trouvent presque pas, sinon jamais à s'appliquer en pratique. De l'avis de la CNPD, le cas de figure du **contrôle temporaire de production ou des prestations du salarié, lorsqu'une telle mesure est le seul moyen pour déterminer le salaire exact** est impra-

34 Voir partie 5.1.1. pour plus d'informations.

ticable. En effet, le seul exemple auquel on pourrait songer est celui des salariés occupés à une chaîne de production qui sont rémunérés en fonction du nombre de pièces fabriquées. Or, il faut noter d'abord qu'il est peu vraisemblable que ce type d'activité et de rémunération existe encore au Grand-Duché de Luxembourg. Ensuite, il faut se rendre à l'évidence qu'il est impossible de déterminer la rémunération mensuelle exacte si la vidéosurveillance ne peut être utilisée que de manière temporaire.

Notons que cette condition de légitimité est pourtant souvent invoquée par les employeurs. Ceci semble tenir du fait que ces derniers comprennent (ou veulent comprendre) que la vidéosurveillance peut être mise en œuvre pour contrôler la production ou les prestations du salarié, sans pour autant réaliser que cette surveillance n'est permise que si elle est **temporaire** et qu'elle est le **seul moyen** pour déterminer la **rémunération exacte**.

En ce qui concerne **les traitements dans le cadre d'une organisation de travail selon l'horaire mobile conformément au Code du Travail**, la CNPD considère qu'il existe d'autres moyens moins attentatoires à la vie privée que l'employeur peut mettre en œuvre pour contrôler les horaires de travail et le temps de présence de ses salariés que la vidéosurveillance. Ainsi, les systèmes de vidéosurveillance utilisés pour vérifier les temps de présence sur le lieu de travail ne sont en principe pas autorisés alors qu'un contrôle des heures de travail par badges est plus efficace et plus protecteur de la vie privée des salariés.

7.1.2.2. Vidéosurveillance de personnes non salariées

Lorsque des personnes non salariées (par exemple : clients, visiteurs, fournisseurs, consultants, etc.) sont filmées par les caméras, l'employeur doit également invoquer et justifier au moins une condition de légitimité de l'article 10 (1) de la loi modifiée du 2 août 2002. Ceci est souvent le cas pour les entreprises ouvertes au grand public et à accès libre, tels que les établissements commerciaux ou administrations par exemple.

Pour les différents critères de légitimation et des exemples, il est renvoyé à la section 5.1.2.

7.1.3. L'autorisation préalable de la CNPD, assortie de conditions

Une autorisation préalable doit être sollicitée auprès de la CNPD par le responsable du traitement voulant mettre en place un dispositif de vidéosurveillance.

Si les finalités d'un traitement de données par caméras vidéo répondent à une ou plusieurs conditions de légitimité, la CNPD analyse ensuite au cas par cas en détail la nécessité et la proportionnalité pour chaque *« zone »* surveillée.

L'analyse de la nécessité d'une vidéosurveillance suppose notamment un examen de moyens alternatifs permettant au responsable du traitement de réaliser les mêmes finalités, mais en utilisant des moyens moins attentatoires à la vie privée des personnes concernées. Selon le groupe de travail *« Article 29 »*[35], ces moyens alternatifs peuvent consister en *« des mesures de prévention, de protection et/ou de sécurité de nature physique et/ou logique ne requérant aucune acquisition d'images, telles que ... dispositifs d'autorisation d'accès, de systèmes d'alarme communs ... »*[36].

Rappelons que le principe de proportionnalité implique que le responsable du traitement doit limiter le traitement à des données adéquates, pertinentes

35 *Groupe de travail réunissant les autorités de protection des données de l'Union européenne.*

36 *Cf. Avis 4/2004 portant sur le traitement des données à caractère personnel au moyen de la vidéosurveillance du groupe de travail « Article 29 », adopté le 11 février 2004 (WP 89, p. 16 à 18).*

7

7. Types de surveillance

et non excessives au regard des finalités à atteindre[37] et que les opérations de traitement ne soient pas disproportionnées.

Dans certaines zones d'installation, les droits des personnes concernées peuvent primer sur la nécessité de mettre en œuvre une vidéosurveillance. Par exemple, l'installation d'une caméra de surveillance dans un bureau où travaille en permanence un salarié doit être considérée comme disproportionnée ou excessive, les droits et libertés fondamentaux des salariés prévalant sur les intérêts poursuivis par l'employeur. De même, l'installation de caméras vidéo dans la cuisine d'un restaurant sera considérée comme disproportionnée et/ou excessive, considérant que tous les salariés employés à la cuisine se trouveront quasiment en permanence sous ces caméras.

Plusieurs jurisprudences sanctionnent au niveau pénal l'absence d'autorisation de la CNPD : **T. Arr. Lux., 24 avril 2008, n°1342/2008 ; T. Arr. Lux., 27 octobre 2008, n°3055/2008 ; T. Arr Lux., 21 octobre 2010, n°3429/2010**.

Dans d'autres décisions est d'abord soulevée la question de la licéité et de l'admissibilité de la preuve des enregistrements d'images en l'absence d'autorisation préalable accordée par la CNPD. En effet, faute d'une autorisation préalable, le traitement de ces images (donc aussi l'utilisation des images comme preuve devant le tribunal) peut potentiellement constituer un délit passible de peines correctionnelles (emprisonnement et/ou amende). L'arrêt qui soulève cette problématique et qui conclut au rejet de telles preuves « illégales » est celui de l'affaire dite « Hôtel des Postes », **T. Arr. Lux., 13 juillet 2006, n°2523/2006**, qui fût confirmé en appel, **C. Appel Lux, 28 février 2007, n°126/07X**. Ces deux arrêts furent cependant cassés par un arrêt de la **Cour de Cassation, Cour de Cass. Lux., 22 novembre 2007, n°57/2007**.

37 Article 4 paragraphe (1) lettre (b) de la loi.

Loin de créer la sécurité juridique que l'on escomptait en la matière, certaines décisions suivent désormais l'argumentation de la Cour de Cassation quant à l'admissibilité et à la licéité de telles images en cas de défaut d'autorisation (voir notamment : **T. Arr. Lux., 26 juin 2008, n°2202/2008 ; T. Arr. Lux., 12 août 2008, n°2614/2008 ; C. Appel Lux., 9 novembre 2010, n°446/10V ; T. Arr. Lux., 1er février 2012, n°534/2012**) alors que d'autres utilisent une argumentation totalement différente pour arriver néanmoins au même résultat (**T. Arr. Lux, 2 février 2009, n°387/2009**, confirmé par **C. Appel Lux., 9 juin 2009, n°288/09V** ; **C. Appel Lux., 16 juin 2009, n°313/09V**).

Reste à relever une jurisprudence intéressante qui conclut à une atteinte au droit à un procès équitable si les images enregistrées sans autorisation de la CNPD auraient été admises en tant que moyen de preuve. Cette conclusion se base notamment sur une analyse détaillée du respect des conditions posées par la loi modifiée du 2 août 2002 et notamment des finalités invoquées par le responsable du traitement ainsi que du respect du droit à l'information préalable des salariés, qui s'en trouve renforcé (**T. Arr. Lux., 16 octobre 2008, n°2925/2008**).

Dans ses autorisations qu'elle délivre en matière de vidéosurveillance, la CNPD peut bien évidemment être amenée à refuser certaines zones, lorsque les conditions de la loi ou le principe de nécessité et de proportionnalité ne sont pas respectés. En usant de son pouvoir d'appréciation, elle fixe par ailleurs dans ses autorisations des conditions et exigences qui peuvent être résumées comme suit :

7.1.3.1. Interdiction d'une surveillance permanente et continue, sauf exceptions rares

En principe, **la loi ne permet pas de soumettre les salariés à une surveillance continue et permanente sur leur lieu de travail**. En effet, les travaux parle-

mentaires précisent à ce sujet que « *la surveillance doit être adaptée au but légitime poursuivi. L'employeur doit recourir aux moyens de surveillance les plus protecteurs de la sphère privée du salarié. Le respect de ce principe de proportionnalité exige que, par exemple, doivent être évitées les surveillances automatiques et continues des salariés*[38] ».

Ainsi par exemple, l'exploitant d'un restaurant n'a pas le droit de surveiller ses salariés à l'intérieur de la cuisine, en invoquant la protection de ses biens. Les salariés seraient soumis à la vidéosurveillance de façon quasi permanente et il est évident qu'une pareille surveillance peut créer une pression psychologique non négligeable pour les salariés qui se sentent et se savent observés, d'autant plus que les mesures de surveillance perdurent dans le temps. Le fait que les salariés ne disposent pas d'un moyen de se soustraire de temps à autre de cette surveillance est également de nature à aggraver cette pression. Une telle surveillance permanente est considérée comme disproportionnée à la finalité recherchée et constitue une atteinte excessive à la sphère privée du salarié occupé à son poste de travail. Dans ce cas, les droits et libertés fondamentaux des salariés doivent prévaloir sur les intérêts poursuivis par l'employeur.

Afin d'éviter une surveillance permanente, il suffit souvent de limiter le champ de vision des caméras à la seule surface nécessaire pour poursuivre les finalités de protection des biens ou de sécurité du personnel. Ainsi, une surveillance par caméras d'une zone caisse(s) par exemple est toujours possible si ces dernières sont configurées de façon à ce que les salariés ne soient pas ciblés. Lesdites caméras doivent être orientées de la façon la moins intrusive possible pour le personnel, c'est-à-dire en limitant leur champ de vision aux seuls endroits où sont manipulés l'argent liquide ou les cartes bancaires, à savoir aux caisses mêmes, aux tiroirs des caisses et, le cas échéant, aux avant-bras des salariés. S'il est vrai que les images provenant de la vidéosurveillance doivent permettre l'identification des auteurs d'éventuelles agressions, il n'est pas pour autant nécessaire de surveiller par caméras les salariés présents derrière le comptoir. Pour cette raison, la CNPD estime qu'il suffit que les caméras soient orientées vers le devant du comptoir, c'est-à-dire qu'elles balisent l'espace d'attente des clients se trouvant devant le comptoir. Les champs de vision des différentes caméras ne doivent donc pas inclure les postes de travail des salariés occupés derrière le comptoir.

Par contre, dans certaines hypothèses, le risque pour la sécurité du personnel peut être d'une importance telle qu'il prime sur la protection de la vie privée de ce dernier. Ainsi, dans la mesure où les hold-up dans les établissements bancaires sont souvent accompagnés de violences, il peut être justifié que certains salariés, en particulier ceux occupés aux guichets-caisses, se trouvent sous une surveillance permanente. La CNPD estime toutefois que le champ de vision des caméras ne doit pas, dans la mesure du possible, cibler un salarié en particulier, et si tel ne peut absolument pas être évité en raison de la configuration des lieux, le salarié en question ne doit pas être filmé de face.

Une surveillance permanente de personnes non salariées pose les mêmes problèmes et n'est pas toujours admise. Ainsi, la CNPD n'autorise pas de filmer l'intérieur d'une salle de restauration comprenant des tables de consommation. Même si un certain risque de vol ou de vandalisme peut exister dans une salle de restauration, celui-ci ne rend pas pour autant une vidéosurveillance automatiquement nécessaire. Force est de constater que les clients présents seront, de façon permanente, soumis à la vidéosurveillance alors qu'ils choisissent un restaurant comme lieu de rencontre pour passer un bon moment autour d'un repas, pour communiquer, se divertir ou se détendre. Or, les clients qui restent dans ce type de lieu pendant un laps de temps plus ou moins long, doivent pouvoir légitimement s'attendre à ne pas être filmés pendant ces moments privés. L'utilisation des caméras dans la salle de restauration comprenant les tables de consommation est susceptible de filmer le comporte-

38 V. doc. parl. 4735/13, p. 22 et 23.

7

7. Types de surveillance

ment de chaque client assis à une table et peut créer une gêne voire une pression psychologique pour les clients qui se sentent observés tout au long de leur présence dans le restaurant. Une telle surveillance permanente est à considérer comme disproportionnée à la finalité recherchée et constitue une atteinte à la sphère privée du client.

La jurisprudence allemande a tranché dans le même sens. Ainsi par exemple, un jugement du 22 avril 2008 du Tribunal administratif (*« Amtsgericht »*) de Hambourg a tranché dans un cas de vidéosurveillance en interdisant à une chaîne commerciale de cafés-brasseries de surveiller la zone clientèle (*« Kundenbereich »*) de ses établissements. Le tribunal a motivé sa décision en soulignant que *« Das Recht auf informationelle Selbstbestimmung verbürgt das Recht des Einzelnen, sich in der Öffentlichkeit frei und ungezwungen bewegen zu dürfen, ohne befürchten zu müssen, ungewollt zum Gegenstand einer Videoüberwachung gemacht zu werden. Ob dieses Recht bei einer Videoüberwachung im öffentlich zugänglichen Raum überwiegt, ist einzelfallsabhängig und situationsbezogen zu beurteilen. (...) Regelmäßig ist die Schutzbedürftigkeit in öffentlich zugänglichen Räumen, in denen sich Menschen typischerweise länger aufhalten und/oder miteinander kommunizieren, besonders hoch einzustufen (...). Dies trifft auf die für Kunden eingerichteten Sitzbereiche, durch die ein längerer Aufenthalt in den Kaffeehausfilialen ermöglicht werden soll, im besonderen Maße zu. (...) Es werden die Persönlichkeitsrechte der sich in den Sitzbereichen länger aufhaltenden Kunden durch eine ständige Videoüberwachung erheblich beeinträchtigt. (...) Hingegen bestehen in den Kundenbereichen keine besonderen Anhaltspunkte für eine Gefahr der Begehung von Straftaten. Insofern kommt in diesen Bereichen dem Interesse der Beklagten an einer effektiven Strafverfolgung auch eine geringere Bedeutung zu. Während also (...), ist die Beobachtung der Kundenbereiche unzulässig (...). Die Beklagte hat daher die Kameras so einzustellen bzw. die Kaffeehäuser so einzurichten, dass die Sitzbereiche nicht von der Videoüberwachung eingefangen werden. »*

7.1.3.2. Interdiction d'enregistrer le son associé aux images

Une surveillance au moyen de caméras vidéo ne doit porter que sur des images à l'exclusion de sons. L'enregistrement du son associé aux images rend la vidéosurveillance encore plus intrusive. Dès lors, ce type d'enregistrements est généralement interdit.

7.1.3.3. Interdiction de surveiller les prestations et les comportements des salariés

Dans toutes ses autorisations, la Commission nationale relève en particulier que la surveillance ne doit pas servir à observer le comportement et les performances des membres du personnel du responsable du traitement en dehors des finalités sur lesquelles est fondée l'autorisation.

Ainsi, un employeur a le droit d'utiliser les images d'un salarié commettant un vol de marchandises et qui proviennent d'un système de vidéosurveillance autorisé sur la finalité de la protection des biens. Or, il n'a pas le droit de prendre des mesures à l'encontre d'un salarié lorsque, au goût de l'employeur, le salarié discute trop longtemps avec un client ou un collègue de travail et que ce comportement est enregistré par le système de vidéosurveillance. Ceci constituerait un détournement de finalité, interdit par la loi et ne devrait, en principe, pas être admis comme moyen de preuve devant les juridictions.

7.1.3.4. Interdiction de filmer les endroits réservés aux salariés pour un usage privé

La CNPD refuse également que les caméras de surveillance filment les endroits réservés aux salariés pour un usage privé ou qui ne sont pas destinés à l'accomplissement de tâches de travail, comme par exemple les toilettes, les vestiaires, le coin fumeurs,

les zones de repos, le local mis à la disposition de la délégation du personnel, la cuisine/kitchenette, etc.

7.1.3.5. Champ de vision limité des caméras filmant les accès intérieurs, extérieurs ou les alentours d'un bâtiment ou d'un site

Les caméras destinées à surveiller un lieu d'accès (entrée et sortie, seuil, perron, porte, auvent, hall, etc.) doivent avoir un champ de vision limité à la surface strictement nécessaire pour visualiser les personnes s'apprêtant à y accéder (accès intérieurs) ; celles qui filment des accès extérieurs ne doivent pas baliser toute la largeur d'un trottoir longeant, le cas échéant, le bâtiment de l'exploitant ou les voies publiques adjacentes.

Les caméras extérieures installées aux abords ou alentours d'un bâtiment doivent être configurées de façon à ne pas capter la voie publique, ni les abords, entrées, accès et intérieurs d'autres bâtiments rentrant éventuellement dans leur champ de vision.

7.1.3.6. Durée de conservation des images limitée

La loi sur la protection des données dispose que les données ne peuvent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées. Pour ce qui est de la vidéosurveillance, la CNPD estime que les images peuvent être conservées en principe jusqu'à 8 jours. Dans certains cas, il est possible de les conserver plus longtemps suivant le cas d'espèce, sans pour autant dépasser un délai de 30 jours.

Les données doivent obligatoirement être détruites après l'écoulement dudit délai. Il est renvoyé au point 5.3.1.3. en ce qui concerne la durée de conservation d'une séquence d'images utilisée comme élément de preuve dans le cadre d'un éventuelle infraction.

7.1.3.7. Aperçu des zones de vidéosurveillance

Si la liste ci-après donne une indication générale dans quelles zones une vidéosurveillance est permise ou non, il convient toutefois de rappeler que la CNPD peut adopter une décision différente en fonction des spécificités du cas d'espèce.

Zones en principe autorisées :

- toutes sortes d'accès, sauf exception (ces zones doivent être limitées à la surface strictement nécessaire) ;
- les locaux de stockage de marchandises / les réserves / les entrepôts / les halls ou hangars de stockage (sauf si des salariés sont affectés en permanence à travailler dans le stock, comme p.ex. des magasiniers) ;
- les espaces ou surfaces de vente / les rayons / la galerie marchande / l'espace d'exposition / l'espace de vente et de conseil (sauf les postes de travail derrière un comptoir) ;
- le parking (intérieur / extérieur / souterrain) ;
- les zones de livraisons ou de chargement / les quais de livraison et de déchargement ;
- la salle informatique / la salle des serveurs ;
- les couloirs (sauf hôtels – situation particulière) ;
- la station de lavage automatique / le carwash,
- les pompes à essence ;
- le coffre-fort / le local sécurisé / les consignes automatiques ;
- les locaux de transport de fonds / le local des convoyeurs de fonds / le local fourgon ;

7

7. Types de surveillance

- les machines de production (uniquement machines) ;
- les installations purement techniques ;
- le local technique / le local de maintenance / le local des compteurs ;
- les archives ;
- les distributeurs automatiques de billets / le guichet automatique bancaire.

Zones en principe non-autorisées :

- la voie publique / le trottoir (autorisés exceptionnellement en fonction de la configuration spécifique des lieux ; le champ de vision ne peut cependant englober qu'une partie extrêmement limitée de la voie publique) ;
- le terrain ou le bâtiment avoisinant ;
- l'intérieur d'un bureau / un poste de travail ;
- la salle ordinaire de réunion ;
- la salle de repos ou de séjour ;
- la salle de sport ;
- les toilettes / les sanitaires / les douches ;
- le bureau de la représentation du personnel ;
- la kitchenette / l'espace fumoir;
- le vestiaire / la salle des casiers ;
- la pointeuse du personnel;
- la salle de consommation d'un établissement de restauration ou d'un débit de boisson ;
- la cuisine / l'intérieur de la cuisine ;
- la cantine / le réfectoire / le bar / la buvette / le café / la terrasse / la caféteria ;
- le comptoir de consommation d'un restaurant (sans caisse) ;
- l'atelier d'un garage / l'atelier de production / l'atelier de travail / l'atelier de montage / démontage.

Zones pour lesquelles l'autorisation de la CNPD varie en fonction des circonstances de l'espèce, de la nature, de la situation ou de la configuration des lieux ; ces zones font généralement l'objet de conditions et de restrictions fixées par la CNPD ; en fonction du cas de figure, ces zones peuvent aussi faire l'objet de refus :

- les alentours immédiats, le parvis ;
- la salle d'attente ;
- la salle de caisse / la salle de comptage de caisse / la salle de traitement des fonds ;
- le hall d'entrée / la réception / la salle d'accueil ;
- les parties communes d'un immeuble ;
- le local « poubelles » / le local à déchets ;
- la cour de récréation (et alentours) ;
- la salle de concerts ;
- la mezzanine, l'atrium ;
- la piscine ;
- le toit du bâtiment ;
- les guichets.

7.2. Surveillance de l'usage des outils informatiques

L'essor des nouvelles technologies de l'information et de la communication dans les entreprises depuis la fin des années 1990 a eu pour conséquence une utilisation croissante des outils informatiques (Internet, messagerie électronique, etc.) par les salariés à des fins professionnelles mais aussi personnelles.

Du point de vue de l'employeur, la surveillance de ces outils est souvent considérée comme une nécessité pour la sécurité de ses systèmes informatiques. Cette « *cybersurveillance* » permet de contrer les potentielles intrusions dans le système informatique ou les virus. Du point de vue du salarié, ce contrôle est souvent vu comme abusif et portant atteinte à sa sphère privée.

Il est évident que le salarié doit exécuter son contrat de travail et qu'il doit respecter son devoir de loyauté vis-à-vis de son employeur. Toutefois, il a également droit au respect de sa vie privée sur son lieu de travail. Ce droit comprend notamment le secret des correspondances.

Ces droits ont été précisés en jurisprudence, notamment avec **CEDH, Halford c. Royaume-Uni, 27.07.1997** et **Cour de Cass. (France), Chambre sociale, 2 octobre 2001, Nikon**.

7.2.1. Quels peuvent être les objectifs poursuivis par l'employeur ?

L'utilisation massive des nouvelles technologies sur le lieu de travail peut constituer une inquiétude pour l'employeur étant donné que l'interconnectivité des réseaux rend le système informatique plus sensible aux attaques extérieures ou à la diffusion d'informations sensibles ou confidentielles.

Ce risque, pouvant mettre en péril les données confidentielles de l'entreprise et de ses salariés, est encore accentué par :

- les usages actuels de l'Internet (blogs, forums, réseaux sociaux, messageries instantanées...) ;
- l'utilisation d'outils portables (clé USB, disque dur externe, ordinateur portable, smartphone...) et
- le concept du BYOD (« *Bring Your Own Device* » – apportez votre appareil personnel), qui est une pratique consistant à utiliser ses équipements personnels (téléphone, ordinateur portable, tablette électronique) dans un contexte professionnel.

L'employeur a donc un intérêt légitime de protéger ses infrastructures informatiques grâce à la surveillance de l'utilisation des outils informatiques au travail. Ses objectifs peuvent notamment être :

- d'éviter que des données confidentielles soient divulguées ou communiquées à des tiers ou, simplement,
- d'avoir un système informatique qui fonctionne normalement (bloquer des codes malveillants, les phénomènes de saturation ou d'engorgement, ...).

S'il tolère généralement l'utilisation des différents outils informatiques à des fins autres que professionnelles, cette utilisation doit rester raisonnable et ne pas affecter la bonne marche de l'entreprise.

7.2.2. Dans quels cas la surveillance des outils informatiques est-elle possible ?

La surveillance de l'usage des outils informatiques des salariés ne peut être mise en œuvre par l'employeur que *« pour les besoins de protection des biens de l'entreprise »*. Celle-ci est en principe la seule condition sur laquelle une telle surveillance peut être légitimée.

Au regard des collaborateurs n'étant pas des salariés de l'employeur, la surveillance est seulement possible si la personne concernée a donné son consentement.

7

7. Types de surveillance

Le consentement susmentionné doit être obtenu de façon libre, spécifique et informée[39]. En l'espèce, le consentement - via une clause, charte ou police prévoyant la surveillance électronique durant leurs activités ou services - des collaborateurs externes devra être recueilli de façon individuelle. La simple mention (de l'existence) d'une telle clause, charte ou police du responsable du traitement est insuffisante.

7.2.3. L'autorisation préalable de la CNPD, assortie de conditions et de recommandations

Entre les intérêts de l'entreprise et le droit des employés au respect de leur vie privée, il appartient à la CNPD de procéder à une analyse détaillée des demandes d'autorisation en vue de la surveillance de l'usage des outils informatiques.

Celle-ci examine d'abord si les objectifs recherchés par l'employeur cadrent avec le critère de la protection des biens.

Les documents parlementaires précisent à cet égard que *« ... relèvent également de la protection des biens de l'entreprise les moyens de surveillance destinés à s'assurer que des virus ne pénètrent pas le réseau d'ordinateurs, que des fichiers professionnels ne soient pas détruits, que le réseau ne soit pas encombré »*[40].

La CNPD considère que *« la protection des biens »* couvre les biens corporels (donc meubles et immeubles) de l'entreprise, mais que cette notion ne comprend pas la protection des intérêts économiques de l'entreprise autres que ceux liés à des biens meubles ou immeubles clairement identifiables. Il ne suffit pas d'invoquer un risque de préjudice financier ou un coût injustifié ou un manque à gagner.

39 Article 2 (c) de la loi modifiée du 2 août 2002.

40 Cf. Doc. parl. n° 4735/13, p. 21.

Les travaux parlementaires indiquent que la sécurité et/ou le bon fonctionnement technique des systèmes informatiques de l'entreprise, ainsi que la protection physique des installations de l'entreprise (par ex. phénomènes d'engorgement, propagation de virus, spoofing, etc.) peuvent être inclus.

Sont également visés des biens incorporels comme les droits de propriété intellectuelle, les secrets d'affaires et de fabrication ainsi que les informations auxquelles est attaché un caractère de confidentialité.

D'autres finalités comme le contrôle du respect du code éthique de l'entreprise (notamment la prévention des comportements illicites et contraires aux bonnes mœurs, la consultation de sites pornographiques, pédophiles et racistes, etc.) et le seul contrôle du respect de la charte informatique (visant par exemple à faire respecter les principes et règles en vigueur dans l'entreprise relatifs à l'usage de l'internet et de la correspondance électronique) ne tombent pas forcément sous la notion de *« protection des biens de l'entreprise »*. Ainsi, il n'est pas permis de contrôler si le salarié surfe sur internet à des fins privées, s'il respecte des règles professionnelles, déontologiques, etc. si ce contrôle s'opère sans rapport avec la protection du système informatique ou avec la protection d'informations confidentielles.

Ensuite, la CNPD analyse la licéité du traitement au regard des principes du secret de la correspondance et de la confidentialité des communications.

Elle se doit également de vérifier la proportionnalité de la surveillance. Le principe de proportionnalité requiert que la méthode de surveillance soit pondérée en fonction des risques concrets que le responsable veut prévenir. Un contrôle général a priori de toutes les données de communication, ainsi qu'un enregistrement de toutes données quelconques dans un but de surveillance, est considéré comme disproportionné.

Les conditions à respecter par l'employeur à cet égard et la manière dont il peut procéder à une surveillance

des outils informatiques sont reprises en détail aux points suivants.

7.2.3.1. Interdiction d'une surveillance permanente

Sauf exception légale, la surveillance permanente des personnes concernées est réputée disproportionnée. Même en cas d'interdiction totale de l'utilisation des outils informatiques à titre privé, l'employeur n'a pas le droit de contrôler l'usage de manière continue, sauf exception légale.

Le principe de proportionnalité exige que les mesures mises en place par l'employeur se limitent à une surveillance ponctuelle et le respect d'une graduation dans l'intensification de la surveillance (*« progressive Kontrollverdichtung »*) qui doit être justifié chaque fois par des indices et soupçons préalablement détectés. Ces vérifications ne peuvent être intensifiées graduellement qu'à l'égard des personnes concernées contre lesquelles les vérifications ponctuelles ont dégagé des indices d'abus ou de comportements irréguliers portant atteinte aux biens de l'entreprise.

Rappelons également les grands arrêts de principe en la matière : **CEDH, Niemietz c. Allemagne, 16.12.1992 et CEDH, Copland, 3 avril 2007**. Selon ces jurisprudences, les activités du salarié sur son lieu de travail et plus particulièrement les courriels et les connexions internet tombent sous la protection de l'article 8 de la Convention européenne des droits de l'homme. Plus précisément, *« 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 »*.

On peut en principe distinguer trois domaines de surveillance informatique, à savoir (a) la surveillance du courrier électronique, (b) la surveillance de l'utilisation d'internet et (c) la surveillance des supports informatiques et des fichiers log.

7.2.3.2. Contrôle de la messagerie électronique

Le secret des correspondances

Tout courriel entrant ou sortant depuis un poste de travail mis à la disposition par l'employeur est présumé être reçu ou envoyé dans le cadre de la relation professionnelle, c'est-à-dire que le destinataire ou l'expéditeur est réputé être l'employeur.

Mais, un tel message n'est pas présumé avoir un caractère professionnel lorsque :

- la mention *« privé »* ou la mention *« personnel »* se trouve dans l'objet du courriel, ou
- l'objet du courriel comporte une mention laissant manifestement supposer qu'il est privé, par exemple *« Vacances Espagne »*.

Dans ce cas, l'employeur ne peut pas ouvrir les courriers électroniques personnels de ses salariés. Ceci constituerait une violation du secret des correspondances ancré dans la Constitution et une infraction pénale, conformément à la loi du 11 août 1982 concernant la protection de la vie privée et la loi du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques et portant modification des articles 88-2 et 88-4 du Code d'instruction criminelle.

La jurisprudence retient aussi que cette interdiction de lire les messages privés s'applique même dans le cas où l'employeur aurait interdit une utilisation des outils informatiques à titre privé (cf. **(FR), Cour de Cass., Chambre sociale, 2 octobre 2001, Nikon**).

La Cour d'Appel du Luxembourg, dans une affaire du 7 avril 2011, a tranché dans le même sens que l'arrêt

7

7. Types de surveillance

Nikon : **C. Appel Lux., 7 avril 2011, n°35507 et 35651 :** *« 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. »*

Notons encore que le principe du secret des correspondances peut cependant être levé dans le cadre d'une instruction pénale ou par une décision de justice.

Contrôle des messages professionnels

Tout ce qui n'est pas identifié comme *« privé »* ou *« personnel »* est réputé être professionnel, de sorte que l'employeur peut y accéder.

Dans une première phase de contrôle, l'employeur peut seulement procéder à une surveillance globale des messages. Ainsi, il peut obtenir des données de trafic et de journalisation comme le volume, la fréquence, la taille, le format de leurs pièces jointes. Ces informations sont contrôlées sans identifier individuellement les salariés.

Dans l'hypothèse où des irrégularités sont constatées, il peut dans une seconde phase passer à l'identification des personnes concernées et contrôler le contenu des courriels professionnels.

Recommandations sur l'utilisation de la messagerie

Pour éviter que l'employeur ne porte atteinte à la confidentialité des messages personnels, la CNPD recommande aux employeurs de suivre les conseils suivants :

- les salariés devraient être invités à distinguer les courriels privés des courriels professionnels en indiquant la nature privée et personnelle dans l'objet des messages et inciter leurs correspondants à faire de même ;
- installer une double boîte de messagerie séparant les messages privés et les messages professionnels ;
- archiver les messages personnels dans un dossier appelé « privé ».

Accès aux courriels pendant l'absence du salarié

Pour assurer la continuité des affaires de l'entreprise pendant l'absence (maladie, congé, etc.) du salarié, la CNPD fait les recommandations suivantes (après que l'employeur ait informé les salariés et les organes représentatifs) :

- mettre en place une réponse automatique d'absence du bureau à l'expéditeur avec indication des personnes à contacter en cas d'urgence ;
- désigner un suppléant qui dispose d'un droit d'accès personnalisé à la messagerie de son collègue : il peut lire et traiter les messages professionnels, mais il ne peut pas lire les messages identifiés comme personnels ;
- transférer à un suppléant tous les messages entrants.

Chaque salarié doit connaître l'identité de son suppléant.

En cas de départ définitif du salarié, il est recommandé que :

- l'employé qui quitte l'entreprise transfère tous les documents professionnels relatifs à des dossiers en cours à une personne prédéfinie (par exemple, son supérieur hiérarchique) ;
- il certifie avoir remis à son employeur tous les documents professionnels ;
- il peut copier les messages électroniques et autres documents de nature privée sur un support privé, puis les effacer des serveurs de l'entreprise ;
- l'employeur s'engage à bloquer tous les comptes informatiques et à effacer la/les boîte(s) aux lettres du salarié dès son départ ;
- les personnes qui enverront un message à l'adresse bloquée sont automatiquement informées de la suppression de l'adresse électronique et reçoivent une adresse alternative.

Ces règles s'inspirent pour la plupart du « Guide relatif à la surveillance de l'utilisation d'Internet et du courrier électronique au lieu de travail »[41] du Préposé fédéral (suisse) à la protection des données et à la transparence. La CNPD se rallie à ces règles et recommandations, notamment dans le cadre de ses autorisations.

Applications jurisprudentielles

La jurisprudence luxembourgeoise considère qu'en l'absence d'autorisation préalable délivrée par la CNPD, le moyen de preuve est inadmissible.

T. Arr. Lux., 25 mai 2012, n°874/2012, (ordonnance en matière de concurrence déloyale). 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 L.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. »*

Trib. travail Lux., 7 mars 2013. Dans une affaire de licenciement, l'employeur verse comme preuve *« un nombre important de courriers électroniques dont certains figurent en annexe de la lettre de licenciement. »* alors qu'il n'a pas demandé d'autorisation auprès de la CNPD pour procéder à une surveillance des e-mails. 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 L.261-1 du Code du Travail. »* Le tribunal a donc écarté des débats les e-mails en cause.

7.2.3.3. Contrôle de l'utilisation de l'Internet

Dans l'environnement du travail, la plupart des employeurs accordent à leurs salariés un accès à Internet pour des raisons professionnelles.

L'employeur peut donc fixer les conditions et limites de l'utilisation d'internet pour des besoins privés et un contrôle doit être possible. Ceci a été confirmé par la jurisprudence française : **(FR), Cass, Chambre**

41 http://www.edoeb.admin.ch/dokumentation/00445/00472/00532/index.html?lang=fr

7

7. Types de surveillance

sociale, 9 juillet 2008[42]. Mais à part l'obligation de devoir demander une autorisation auprès de la CNPD, l'employeur doit également informer clairement et préalablement les salariés sur les dispositifs et les modalités de contrôle mis en place, sinon il s'agirait d'une surveillance cachée à leur insu.

Il ne peut pas surveiller individuellement un salarié sans avoir, au préalable, procédé à une surveillance globale et non personnelle. Ainsi, il peut faire dresser une liste d'adresses de sites consultés de façon globale sur une certaine période, sans identifier les auteurs des consultations. S'il a des indices sur une utilisation d'Internet préjudiciable pour l'entreprise en repérant une durée anormalement élevée de présence sur Internet ou la mention d'adresses de sites suspects, il pourra alors prendre les mesures de contrôle appropriées, et passer alors, dans un second stade, à une surveillance individualisée.

La CNPD recommande la mise en place de moyens de protection préventifs compte tenu des risques de virus que présentent ces accès, comme par exemple, le filtrage de sites non autorisés, l'interdiction de téléchargements de logiciels ou l'interdiction de se connecter à des forums de discussion.

7.2.3.4. Contrôle des supports informatiques et des fichiers de journalisation

De façon générale, tous les documents et fichiers créés par un salarié sont censés être de nature professionnelle. Toutefois, le salarié peut, dans les limites du raisonnable, créer des documents ou fichiers qu'il identifie comme étant privé (principe confirmé en jurisprudence). Selon l'arrêt Cathnet-Science, **(FR), Cour de Cass., Chambre sociale, 17 mai 2005**, 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 ».

À nouveau, la surveillance des supports informatiques et des fichiers de journalisation ne doit pas se faire sous forme d'analyse individualisée mais doit être graduée dans le rythme et l'envergure des données contrôlées. En d'autres mots, l'employeur n'a pas le droit de procéder immédiatement à un contrôle individuel sans avoir procédé auparavant à un contrôle global où des irrégularités ont été détectées.

En ce qui concerne les fichiers ou documents identifiés comme privés, l'employeur ne peut pas y accéder sans la présence du salarié concerné. Ce dernier doit avoir la possibilité de s'opposer à l'ouverture d'un fichier privé et doit être informé de cette possibilité au moment du contrôle.

La CNPD recommande donc que l'employeur prenne des mesures destinées à assurer que les documents électroniques de l'entreprise soient accessibles pendant l'absence du salarié sans qu'il soit nécessaire d'ouvrir les dossiers « personnels ou privés » du salarié.

Enfin, il est recommandé qu'à la fin de son emploi, le salarié puisse obtenir une copie des documents conservés dans son fichier privé et qu'il ait la possibilité d'effacer ses dossiers personnels, le cas échéant, en présence d'un représentant de l'employeur.

Applications jurisprudentielles

C. Appel Lux., 3 mars 2011, n°35462 : Un salarié reçoit sur son adresse e-mail privée un document intitulé « brainstorming.doc » qui est enregistré sur le disque dur de son ordinateur professionnel. Ledit document est ensuite « restauré » sur l'ordinateur par l'employeur, alors qu'il y a été supprimé. Le salarié estime que l'employeur a violé le secret des correspondances. La Cour rappelle, en se référant à la jurisprudence de

42 *« 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 ».*

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 à priori aucun caractère privé »* et qu'il n'y a pas lieu de faire abstraction du document, c'est-à-dire que le document peut servir comme preuve.

7.2.3.5. Obligation d'informer les salariés concernés

L'employeur doit informer ses salariés de ce qu'il tolère comme usage à des fins personnelles des outils informatiques ainsi que des dispositifs mis en place et des modalités de contrôle de ces outils. En d'autres termes, il doit mettre au courant les salariés dans quelle mesure il les autorise à utiliser une messagerie électronique et/ou à surfer sur Internet et/ou à créer et à disposer de fichiers personnels.

Sans être exhaustif, il peut s'agir des informations suivantes :

- l'utilisation de ces outils à des fins privées (les périodes et les durées d'utilisation, le mode de stockage des informations sur le disque dur,...) ;
- les raisons et les objectifs du contrôle, la nature des données collectées, l'étendue et les circonstances des contrôles, les destinataires des données ;
- la mise en place d'outils bloquant des sites Internet et/ou des messages en chaîne ou des fichiers trop lourds ;
- le mode de collecte et l'utilisation des données issues de la surveillance ;
- les personnes autorisées à utiliser les données issues de la surveillance et dans quelles circonstances ;
- la durée de conservation des données issues de la surveillance ;
- les décisions pouvant être prises par l'employeur lors d'un contrôle ;
- le rôle des représentants des salariés dans la mise en œuvre de la politique de surveillance ;
- les modalités du droit d'accès des salariés à leurs données.

Dans un souci de transparence et de loyauté dans les relations de travail, la CNPD recommande que l'employeur adopte une charte, un règlement interne ou tout autre document relatif à l'utilisation et aux modalités de contrôle des outils informatiques mis à disposition des salariés.

Les travailleurs et les collaborateurs externes susceptibles d'être exposés à la surveillance de leur utilisation des outils informatiques et communications électroniques doivent bien évidemment aussi en être préalablement informés.

7.2.3.6. Durée de conservation limitée

Pour la surveillance des outils informatiques, la CNPD considère en règle générale qu'un délai de conservation des données issues de la surveillance de 6 mois est suffisant.

Dans le cadre de la transmission des données aux autorités judiciaires compétentes, les données peuvent toutefois être conservées au-delà du délai susmentionné.

Les limites de conservation susmentionnées ne s'appliquent pas aux documents commerciaux et comptables qui peuvent être conservées jusqu'à l'expiration des délais de prescription applicables.

7

7. Types de surveillance

7.2.3.7. Rôle des administrateurs systèmes / réseaux informatiques

Les administrateurs qui doivent veiller à assurer le fonctionnement normal et la sécurité des réseaux et systèmes informatiques sont conduits, de par leurs fonctions mêmes, à avoir accès à l'ensemble des informations relatives aux utilisateurs (messagerie, connexions à internet, fichiers « logs » ou de journalisation, etc.) y compris celles qui sont enregistrées sur le disque dur du poste de travail.

Ils doivent donc être soumis à une obligation renforcée de secret professionnel ou de discrétion professionnelle. De manière générale, dans le cadre de ses autorisations, la CNPD adopte et prend à son compte certaines remarques et exigences élaborées par la Commission Nationale de l'Informatique et des Libertés française (CNIL) et retient que : « *l'accès aux données enregistrées par les employés dans leur environnement informatique - qui sont parfois de nature personnelle - ne peut être justifié que dans les cas où le bon fonctionnement des systèmes informatiques ne pourrait être assuré par d'autres moyens moins intrusifs.*

De plus, aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations dont les administrateurs de réseaux et systèmes peuvent avoir connaissance dans l'exercice de leurs fonctions ne saurait être opérée, d'initiative ou sur ordre hiérarchique.

De même, les administrateurs de réseaux et systèmes, généralement tenus au secret professionnel ou à une obligation de discrétion professionnelle, ne doivent pas divulguer des informations qu'ils auraient été amenés à connaître dans le cadre de leurs fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Ils ne sauraient non plus être contraints de le faire, sauf disposition législative particulière en ce sens.[43] »

7.2.3.8. Fichiers de journalisation

Les fichiers de journalisation des connexions destinés à identifier et enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations constituent des mesures favorisant la sécurité et la confidentialité des données à caractère personnel. Celles-ci ne doivent pas être accessibles à des tiers non autorisés ni utilisées à des fins étrangères à celles qui justifient leur traitement. Ils n'ont pas pour vocation première le contrôle des utilisateurs.

Comme les fichiers de journalisation constituent des mesures favorisant la sécurité et la confidentialité, ils ne sont pas à considérer comme un traitement à des fins de surveillance.

En revanche, la mise en œuvre d'un logiciel d'analyse des différents journaux (applicatifs et systèmes) permettant de collecter des informations individuelles poste par poste pour contrôler l'activité des utilisateurs, doit être considéré comme un traitement à des fins de surveillance avec toutes les conséquences que cela comporte telles que la nécessité d'une autorisation de la Commission nationale, la limitation des mesures au critère de légitimation de la protection des biens et la proportionnalité des contrôles éventuels.

43 http://www.ladocumentationfrancaise.fr/rapports-publics/044000175/

7.3. Enregistrement des conversations téléphoniques

Dans le cadre de son activité commerciale, un employeur peut être amené à procéder à l'enregistrement des conversations téléphoniques de ses salariés et de leurs correspondants.

Cette mesure de surveillance est notamment pratique courante dans le secteur financier, où les professionnels enregistrent les conversations téléphoniques en vue de se procurer une preuve des transactions commerciales (p.ex. opérations de bourse). Si cette finalité était d'ailleurs la seule pour laquelle le traitement pouvait être autorisé jusqu'en 2007, le législateur a depuis lors élargi le champ d'application des enregistrements de communication électroniques en général et des enregistrements téléphoniques en particulier, en rajoutant comme finalité aussi la preuve de *« toute autre communication commerciale »*, en visant par exemple les enregistrements des conversations téléphoniques effectués par les *« call center »*, les *« Help-desk »*, les services après-vente, etc.

7.3.1. Quels peuvent être les objectifs poursuivis par l'employeur ?

Dans le cadre des activités journalières des banques, des établissements financiers et de certaines autres sociétés commerciales, les enregistrements téléphoniques poursuivent généralement les finalités suivantes :

- la nécessité de se prémunir d'une preuve des transactions commerciales ou des communications commerciales en cas de litige,
- l'acquisition des données sur les négociations, opérations, arbitrages, transactions, etc.,
- la vérification des engagements commerciaux fixés par téléphone,
- la confirmation des détails d'un ordre de bourse/d'une instruction (vente, achat, souscription, livraison, etc.),
- la réécoute des instructions,
- la résolution des malentendus.

7.3.2. Dans quels cas les enregistrements téléphoniques sont-ils possibles ?

Le principe est celui de la confidentialité des communications et résulte d'une continuité dans les textes légaux nationaux et internationaux :

- article 28 de la Constitution : *« Le secret des lettres est inviolable (...) »*,
- l'article 8 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du 4 novembre 1950 : *« Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »*,
- la Charte des droits fondamentaux de l'Union Européenne proclamée à Nice le 7 décembre 2000 a retenu la même formule, mais en substituant le terme de *« communication »* à celui de *« correspondance »*,
- la loi du 11 août 1982 concernant la protection de la vie privée,
- la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement de données à caractère personnel qui prévoit, sous réserve de conditions restrictives, la possibilité d'effectuer un traitement de données personnelles à des fins de surveillance dont, entre autres, l'enregistrement de conversations téléphoniques,

7

7. Types de surveillance

- la loi modifiée du 30 mai 2005 relative aux dispositions spécifiques de protection de la personne à l'égard du traitement des données à caractère personnel dans le secteur des communications électroniques (transposant en droit interne luxembourgeois la directive 2002/58/CE dite directive *« vie privée et communications électroniques »*) qui prévoit la possibilité d'enregistrements des communications lorsqu'ils sont effectués *« dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale »*.

Les textes légaux nationaux et internationaux témoignent ainsi de l'importance accordée à la confidentialité des communications. Il a par ailleurs été précisé par la jurisprudence de la CEDH que les appels téléphoniques rentrent indubitablement dans la notion de *« vie privée »* et de *« correspondance »* (cf. **CEDH, Halford c. Royaume-Uni, 25 juin 1997,** idem, **CEDH, Copland c. Royaume-Uni, 3 avril 2007)**. Si le législateur a rendu possible une surveillance par enregistrement des conversations téléphoniques, c'est sous réserve des conditions restrictives qui concilient les intérêts des personnes concernées en matière de protection de la vie privée avec ceux que peuvent poursuivre les responsables de traitement.

Les enregistrements des conversations téléphoniques sur le lieu du travail peuvent donc uniquement servir de preuve d'une transaction commerciale ou d'une « autre » communication commerciale, en cas de survenance d'éventuelles contestations ou litiges. *Ne sont donc pas autorisés* les enregistrements des conversations privées ainsi que les enregistrements dont les finalités ne rentrent pas dans les prévisions légales, comme par exemple :

- l'exercice d'un contrôle des performances professionnelles des salariés,
- l'utilisation des données recueillies à des fins d'évaluation des salariés,
- le contrôle de la qualité des conversations téléphoniques.

7.3.3. L'autorisation préalable de la CNPD, assortie de conditions et de recommandations

Dans chacune de ses autorisations, la CNPD fixe une série de conditions et de restrictions qui découlent des principes généraux de la législation sur la protection des données.

Ainsi, la CNPD examine au cas par cas si les objectifs recherchés par l'employeur correspondent bien aux cas légitimes prévus par la loi. Elle doit également vérifier la nécessité et la proportionnalité des enregistrements téléphoniques.

7.3.3.1. Interdiction de l'enregistrement systématique de tous les postes

Seuls les postes téléphoniques des départements déterminés à l'avance par l'employeur, essentiels à l'activité commerciale de l'entreprise et à partir desquels des communications commerciales sont effectuées, seront autorisés (p.ex. : salle de marchés, département Private Banking, Gestion de fonds, Help Desk, etc.). La CNPD considère en effet que l'enregistrement systématique des conversations opérées à partir de tous les postes de l'entreprise est disproportionné par rapport à la finalité qui consiste à recueillir la preuve d'une transaction ou d'une communication commerciale. Les postes téléphoniques des départements qui semblent a priori étrangers à cette finalité ne seront en principe pas autorisés.

7.3.3.2. Mise à disposition d'une ligne spécifique non surveillée

Au sein des départements autorisés, l'employeur devra mettre à disposition, pour les salariés ainsi que pour les correspondants externes, une ligne téléphonique non surveillée, afin d'établir une communication téléphonique non soumise à enregistrement pour les conversations privées/personnelles.

7.3.3.3. Information des salariés et des tiers

La surveillance des conversations téléphoniques concerne tant les salariés du responsable du traitement que leurs correspondants. À ce titre, la CNPD distingue entre les correspondants qui sont des professionnels relevant d'un secteur dans lequel il est d'usage professionnel licite d'enregistrer les conversations téléphoniques (tels que les acteurs du secteur financier comme les boursiers) et les correspondants qui sont des personnes privées (p.ex. les clients).

Les obligations du responsable du traitement varient dès lors en fonction d'une de ces catégories de personnes :

- **En ce qui concerne les salariés**, ceux-ci doivent obligatoirement être informés de la surveillance (ainsi que, le cas échéant, leurs organismes de représentation). Cette obligation d'information découle non seulement des dispositions spécifiques de la loi modifiée du 30 mai 2005, mais également des dispositions générales de la loi modifiée du 2 août 2002 en matière de surveillance des salariés.
- Il s'agit ici d'une obligation d'information préalable *« des parties aux transactions »* (par message préalable ou convention spécifique), faute de quoi l'enregistrement pourra le cas échéant être considéré comme nul en tant que moyen de preuve devant un tribunal. Voir en ce sens : **(LU) C.A. Luxembourg, 24 octobre 2002, n°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 »*.
- **En ce qui concerne les tiers non professionnels** (tels que les clients privés), la loi modifiée du 30 mai 2005 a introduit une disposition (article 4, paragraphe 3, lettre d) qui prévoit que le responsable du traitement n'est plus tenu d'obtenir le consentement des parties à la communication pour en effectuer l'enregistrement, dans l'hypothèse unique où cet enregistrement *« est effectué dans le cadre des usages professionnels licites, afin de fournir la preuve d'une transaction commerciale ou de toute autre communication commerciale »*. En contrepartie, cette même disposition de la loi soumet très clairement le responsable du traitement à l'obligation d'informer au préalable les parties correspondantes sur les conditions d'enregistrement des communications, les raisons pour lesquelles les communications sont enregistrées ainsi que de la durée maximale de conservation des données.

  Dès lors, afin d'attirer l'attention des correspondants tiers (notamment les clients) de façon suffisamment claire sur les conditions d'enregistrement des communications, la CNPD estime que cette information préalable doit être fournie à ceux-ci par la signature d'une convention spécifique relative à l'utilisation du service téléphonique proposé (et ne pas être *« noyée »* dans les conditions générales). Dans cette hypothèse, le responsable du traitement doit également prendre toutes les mesures organisationnelles et techniques nécessaires, afin d'éviter que des communications étrangères à toute transaction ou communication commerciale ou des communications avec des non-clients ou des

7

7. Types de surveillance

clients potentiels ne puissent être enregistrées. À défaut de pouvoir respecter ces deux conditions simultanément, la CNPD estime nécessaire que lors de chaque entretien téléphonique soumis à enregistrement, les correspondants tiers soient spécifiquement rendus attentifs à l'enregistrement, moyennant diffusion d'un message automatisé ou non au début de l'appel.

- **En ce qui concerne les professionnels relevant d'un secteur dans lequel il est d'usage professionnel licite d'enregistrer les conversations téléphoniques** (tels que les courtiers, gestionnaires de fonds, salariés d'autres banques, etc.), une information préalable au début de chaque appel n'est pas nécessaire.

7.3.3.4. Durée de conservation limitée

La CNPD estime que le responsable du traitement pourra conserver les données relatives aux enregistrements téléphoniques pour une période maximale de dix ans à partir de la date d'enregistrement. Cette durée s'aligne sur le délai décennal de la prescription commerciale applicable aux types de transactions et communications commerciales pour lesquelles les enregistrements téléphoniques peuvent servir de preuve.

7.4. Les systèmes biométriques

Les données biométriques peuvent se définir comme *« des propriétés biologiques, des aspects comportementaux, des caractéristiques physiologiques, des caractéristiques vivantes ou des actions reproductibles lorsque ces caractéristiques et/ou actions sont à la fois propres à cette personne physique et mesurables, même si les méthodes utilisées dans la pratique pour les mesurer techniquement impliquent un certain degré de probabilité »* [44]. Parmi les exemples de données biométriques figurent les empreintes digitales, la structure du système veineux des doigts de la main, mais aussi la dynamique de frappe sur un clavier.

Les données biométriques ne sont pas des données à caractère personnel comme les autres. En effet, elles ne sont pas attribuées par un tiers ou choisie par la personne. Elles permettent d'identifier de manière définitive et indubitable un individu à partir de certaines caractéristiques uniques à son propre corps. Le mauvais usage ou le détournement de telles données peut donc avoir des conséquences graves[45].

Comme elles permettent d'identifier de façon immuable une personne par ses caractéristiques physiologiques ou comportementales, certains employeurs peuvent désirer avoir recours à des traitements comportant des données biométriques, comme nous le détaillons au point 7.4.1.

C'est également pour cette raison que les systèmes utilisant des données biométriques comportent des risques beaucoup plus élevés que, par exemple, un dispositif de vidéosurveillance (non biométrique). En effet, il a été démontré qu'il peut être très facile de reproduire des données biométriques telles que les empreintes digitales à l'insu des personnes concernées, simplement à partir des traces que celles-ci laissent (par exemple sur un verre) ! Or, à l'inverse d'un mot de passe par exemple, une donnée biométrique ne peut jamais être réinitialisée.

44 Avis 4/2007 du 20 juin 2007 sur le concept de données à caractère personnel du groupe de travail « Article 29 » sur la protection des données, p. 9, disponible à l'adresse : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf

45 « Biométrie : des dispositifs sensibles soumis à autorisation de la CNIL », article disponible à l'adresse : http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/biometrie-des-dispositifs-sensibles-soumis-a-autorisation-de-la-cnil/

C'est pourquoi les traitements comportant des données biométriques nécessaires au contrôle de l'identité des personnes sont soumis, aux termes de l'article 14 paragraphe (1) lettre (f) de la loi du 2 août 2002, à l'autorisation préalable de la Commission nationale. Au point 7.4.3., nous présentons les conditions dans lesquelles la Commission nationale autorise ou non de tels traitements de données.

7.4.1. Quels peuvent être les objectifs poursuivis par l'employeur ?

Le recours à des systèmes biométriques par l'employeur permet à celui-ci de contrôler l'identité des personnes. Cet objectif peut certes être atteint par d'autres procédés, tels que l'emploi de badges ou de mots de passe. Mais tandis que les badges et mots de passe peuvent être très facilement échangés ou permutés, les systèmes biométriques permettent d'identifier sans équivoque la personne qui désire accéder à un local déterminé. Le renforcement des mesures de sécurité aux accès à certains locaux identifiés, ou à des serveurs informatiques par exemple, constitueront donc des exemples de finalités qui pourront être invoquées par l'employeur qui désire avoir recours à des systèmes biométriques.

7.4.2. Dans quel cas les systèmes biométriques sont-ils possibles ?

L'employeur devra invoquer au moins une condition de légitimité éligible de l'article L.261-1(1) du Code du Travail, à savoir :

- le contrôle des horaires de travail ;
- la protection des biens ;
- la sécurité et santé des travailleurs.

Contrôle des horaires de travail

L'employeur entend par exemple mettre en place un système de pointage au moyen d'un lecteur biométrique, qui présente l'avantage par rapport aux badges qu'il permet d'éviter certains abus qui consistent à s'échanger les badges entre collègues de travail afin de modifier leurs heures d'entrée et de sortie des locaux de l'employeur.

Protection des biens

L'employeur souhaite renforcer la protection de certaines zones de ses locaux contenant des biens ou des données particulièrement sensibles à ses yeux, telles que la salle des serveurs. Il veut ainsi garantir que seuls les employés autorisés à y avoir accès puissent y rentrer, garantie qui n'apparaît pas aussi forte avec d'autres moyens de contrôle d'accès.

Sécurité et santé des travailleurs

Il peut par exemple s'agir du cas de figure où l'employeur souhaiterait limiter l'accès à un local contenant des produits dangereux pour la santé (virus, produits chimiques, etc.) et à manipuler avec grande précaution par les seules personnes habilitées pour ce faire au sein d'un laboratoire.

7.4.3. L'autorisation préalable de la CNPD

Etant donné que les données biométriques comportent des risques élevés en matière de protection des données, la Commission nationale estime que conformément au principe de proportionnalité, un employeur ne doit avoir recours à un système biométrique que si cela est absolument nécessaire pour réaliser ses finalités, et pas seulement parce que cela serait simplement « utile », « opportun » ou plus « pratique » pour l'employeur que des systèmes plus traditionnels, tels que des mots de passe ou des badges d'accès.

7

7. Types de surveillance

La proportionnalité implique que l'employeur doit limiter le traitement à des données adéquates, pertinentes et non excessives au regard des finalités à atteindre. Pour vérifier si cette condition de proportionnalité est respectée, la CNPD opère une double distinction entre les systèmes utilisant des données biométriques qui laissent des traces et celles qui n'en laissent pas, d'une part, et entre les systèmes qui stockent de façon centralisées les données biométriques dans une base de données et ceux qui ne les stockent que de façon décentralisée, par exemple dans un badge.

Données biométriques laissant ou non des traces

Les données biométriques qui laissent des traces, telles que les empreintes digitales, sont considérées comme potentiellement les plus attentatoires aux libertés individuelles car les traces peuvent être capturées et reproduites à l'insu des personnes concernées. Le fait que la donnée biométrique soit convertie par un algorithme en un numéro, communément appelé gabarit, n'enlève pas ce risque.

Les données biométriques qui ne laissent pas de traces, comme par exemple le contour de la main, la rétine, le réseau veineux d'une main ou d'un doigt, ne présentent pas les mêmes dangers que celles qui laissent des traces.

Données biométriques stockées ou non de façon centralisée

Les données biométriques qui sont stockées dans une base de données centralisée à laquelle d'autres personnes que l'employé lui-même a accès présentent plus de risques que celles stockées dans un support individuel (par exemple, sauvegardé sur un badge ou une carte magnétique) dont l'employé a la seule maîtrise.

Sur base de cette double distinction, la CNPD autorise, au stade actuel des technologies utilisées :

- les systèmes contenant des données biométriques qui ne laissent pas de traces (par exemple, le contour de la main, le réseau veineux), peu importe si les données biométriques sont stockées de façon centralisée ou non. En effet, ceux-ci 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 (un badge, une carte magnétique), peu importe qu'elles laissent des traces (par exemple les empreintes digitales) ou non.

Par contre, la CNPD refuse en principe les systèmes comportant des données biométriques laissant des traces, telles que les empreintes digitales, lorsque ces données ou les gabarits sont stockés dans une base de données centralisée. De manière tout à fait exceptionnelle toutefois, de tels traitements peuvent être autorisés si le requérant justifie de raisons impérieuses de sécurité ou de protection de l'activité exercée dans les locaux à protéger, et qu'en outre, l'accès est circonscrit à un nombre très limité de personnes autorisées à accéder à une zone délimitée représentant ou contenant un enjeu majeur dépassant l'intérêt strict du responsable du traitement. Ces cas demeurent cependant très rares en pratique.

De façon générale, la CNPD recommande de choisir un système qui fonctionne avec des données biométriques qui ne laissent pas de traces (par exemple, le contour de la main ou le réseau veineux, comme expliqué ci-avant), qui sont tout aussi fiables que les systèmes avec empreintes digitales et répondent aussi aux finalités poursuivies.

Durée de conservation limitée des données

La loi sur la protection des données dispose que les données ne peuvent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées.

Une durée limitée de conservation de données constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalités.

Pour ce qui est des données biométriques, la CNPD estime que leur durée de conservation ne doit pas être supérieure au temps pendant lequel la personne concernée est habilitée à pénétrer dans les zones délimitées.

Par ailleurs, la Commission nationale estime que le requérant peut conserver les données relatives aux contrôles d'accès, c'est-à-dire l'historique des passages, pendant trois mois au maximum à compter de leur enregistrement.

Enfin, les données relatives au contrôle des horaires de travail ne doivent pas être conservées au-delà de trois ans pour les travailleurs salariés et assimilés, ou au-delà de cinq ans pour les agents publics.

En cas d'incident, les données relatives aux accès ou au contrôle des horaires de travail ne font pas l'objet de l'obligation de destruction au bout de trois mois respectivement trois ou cinq ans dans le cadre de la transmission des données aux autorités judiciaires compétentes pour constater ou pour poursuivre une infraction pénale.

7.5. Dispositifs de géolocalisation

Les systèmes plus « traditionnels » de géolocalisation du véhicule professionnel utilisé par le salarié sont de plus en plus remplacés par des dispositifs de géolocalisation portables, portés parfois même sur le corps des salariés : boîtiers GPS, badges et applications sur smartphone permettent désormais de localiser à tout moment les salariés. L'employeur peut donc positionner leurs déplacements dans le temps ainsi que dans l'espace.

Ces technologies permettent au responsable de traitement de collecter et de traiter des données à caractère personnel telles que le temps de travail, l'identité du conducteur, le nombre de pauses effectuées, le kilométrage parcouru ou encore les itinéraires empruntés. Mais ces nouveaux systèmes, qui permettent plein de fonctionnalités nouvelles, comme la possibilité de détecter la perte de verticalité, présentent aussi de nouveaux dangers pour la vie privée des salariés.

Au regard du caractère particulièrement intrusif d'une telle surveillance pour la vie privée des salariés, tout dispositif de géolocalisation doit faire l'objet d'une autorisation préalable de la CNPD et l'employeur doit respecter un certain nombre d'exigences légales et pratiques.

7.5.1. Quels peuvent être les objectifs poursuivis par l'employeur ?

Avant l'installation d'un dispositif de géolocalisation, l'employeur devra définir les objectifs qu'il souhaite atteindre en recourant à un tel système.

Dans bien des cas il peut s'agir des finalités suivantes :

- optimisation du processus de travail par une meilleure allocation des moyens disponibles (par exemple, envoi du véhicule le plus proche du lieu d'intervention, gestion de la flotte de véhicules,...) ;
- assurer le suivi de marchandises en raison de leur nature particulière (matières dangereuses, denrées alimentaires) ;
- établir le suivi et la constitution de preuve de l'exécution d'une prestation liée à l'utilisation du véhicule (par exemple, intervention sur réseau routier, collectes des ordures ménagères,...) dans le souci de facturation des prestations aux clients ;

7

7. Types de surveillance

- contribuer à la sécurité des biens (véhicules, matériels transportés) ;
- assurer la sécurité des salariés ;
- prévenir et détecter la survenance d'atteintes à l'intégrité physique des personnes concernées ;
- suivre le temps de travail des salariés (lorsque cela ne peut être opéré par d'autres moyens) ;
- pouvoir alerter en temps utile les forces de l'ordre ou les services de secours en cas d'infraction ou d'accident ;
- etc.

Au regard des finalités invoquées par l'employeur, la CNPD vérifiera d'une part, si ces finalités sont légitimées par au moins un des cas prévus par la loi et d'autre part, si la géolocalisation est nécessaire et proportionnelle par rapport aux objectifs que souhaite atteindre l'employeur.

7.5.2. Dans quels cas la géolocalisation est-elle possible ?

Il appartient à la CNPD de vérifier si les finalités invoquées par l'employeur correspondent à au moins un des cas prévus par la loi.

En effet, la surveillance des salariés sur le lieu du travail n'est possible que si elle est nécessaire :

- pour les besoins de sécurité et santé des salariés,
- pour les besoins de protection des biens de l'entreprise,
- pour le contrôle du processus de production portant uniquement sur les machines, ou
- pour les traitements dans le cadre d'une organisation de travail selon l'horaire mobile conformément au Code du Travail.

Sécurité et santé des travailleurs

Le recours à un système de géolocalisation peut être considéré comme légitime s'il permet de garantir la sécurité des salariés. Ce critère de légitimation est en principe accepté par la CNPD lorsque l'activité des salariés du requérant est de nature à porter atteinte à leur intégrité physique, soit parce que les fonctions qu'ils exercent sont périlleuses, soit parce que les salariés pourraient faire l'objet d'attaques physiques en raison par exemple de la valeur des biens qu'ils ont sous leur garde, c'est-à-dire qu'ils transportent eux-mêmes ou dans leur véhicule.

Ce critère peut, par exemple, être invoqué par une société de transport de fonds. Au regard de l'importance des fonds et des valeurs qu'ils ont sous leur garde, il est en effet légitime que l'employeur soit en mesure de déceler tout problème durant leur parcours et permettre notamment d'avertir le plus rapidement possible les forces de l'ordre en cas de problème.

Protection des biens de l'entreprise

Dans ce cas de figure, l'employeur entend protéger les biens de son entreprise, c'est-à-dire les véhicules mis à la disposition de ses salariés mais également les biens que ceux-ci transportent (marchandises, liquidités, outillages,...). En cas d'attaque ou de vol du véhicule, il sera possible pour le responsable du traitement de pister le véhicule concerné et les biens dérobés. Les autorités policières pourront donc rapidement localiser les déplacements exacts du véhicule et éventuellement intercepter les auteurs du vol.

Contrôle du processus de production portant uniquement sur les machines

Il ressort des travaux parlementaires de la loi qu'initialement, le législateur avait uniquement envisagé sous couvert de cette condition de légitimation l'hypothèse de la surveillance incidente des salariés au cours de la surveillance principale d'un système industriel de production mécanisé de type chaîne de

production, dans le but d'en contrôler le bon fonctionnement.

La CNPD estime cependant qu'il est possible d'étendre cette condition de légitimité aux contrôles des prestations de service au moyen d'un système de géolocalisation. En effet, ce cas d'ouverture est proche de l'hypothèse initialement envisagée par le législateur car dans les deux cas, la surveillance des salariés est à considérer comme accessoire. Le but principal recherché par la surveillance est, dans les deux hypothèses, le contrôle de l'infrastructure matérielle, des machines et des outils mis à disposition par l'employeur dans le cadre de son activité professionnelle. Les intérêts recherchés par les employeurs sont donc similaires, que le processus de travail soit de production industrielle ou en matière de fourniture de prestations de service.

Traitement nécessaire dans le cadre d'une organisation de travail selon l'horaire mobile

L'organisation du travail selon l'horaire mobile est un système d'organisation qui offre aux salariés la faculté d'aménager l'horaire et la durée de travail selon leur convenance personnelle dans le respect de plages horaires prédéfinies des besoins de service.

La CNPD considère qu'un système de géolocalisation peut être utilisé pour suivre le temps de travail des salariés. En effet, partant du postulat que l'atteinte à la vie privée des salariés est strictement la même quel que soit le mode d'organisation de travail choisi par l'employeur (horaire mobile ou fixe), la CNPD ne voit pas d'objection à y recourir dans le cadre d'une organisation de travail selon l'horaire mobile. Toutefois, avant toute autorisation, elle ne manquera pas de vérifier si le suivi ne peut pas être réalisé par d'autres moyens moins intrusifs pour les salariés. De plus, une telle surveillance ne sera qu'admise que si un système d'horaire mobile est effectivement présent dans l'entreprise, avec des créneaux prédéfinis, etc.

Par ailleurs, il y a lieu de souligner qu'un système de géolocalisation ne se justifie pas si le salarié est libre d'organiser son travail comme il l'entend (par exemple, un VRP).

7.5.3. L'autorisation préalable de la CNPD, assortie de conditions et de recommandations

Une autorisation préalable doit être sollicitée auprès de la CNPD par le responsable du traitement voulant mettre en place un dispositif de géolocalisation.

Outre l'existence d'une ou plusieurs conditions de légitimité, la CNPD vérifiera si le recours à la géolocalisation est nécessaire et proportionnel par rapport aux finalités invoquées par l'employeur.

Les systèmes de géolocalisation soulèvent la délicate question du niveau de contrôle qu'il est admissible de faire peser sur un salarié pendant tout son temps de travail, voire de la frontière entre travail et vie privée.

Le principe de proportionnalité implique que le responsable du traitement doit limiter le traitement à des données adéquates, pertinentes et non excessives au regard des finalités à atteindre[46] et que les opérations de traitement ne soient pas disproportionnées.

Comme on l'a vu auparavant, ces nouveaux systèmes présentent clairement de nouveaux dangers pour la vie privée des salariés. Or, les droits de l'employeur doivent se concilier avec les droits et libertés des salariés. Les dispositions légales en matière de protection des données ne doivent donc pas être dissociées de celles du droit du travail. Il en résulte que la surveillance doit être la moins intrusive possible et que le salarié doit conserver le droit de pouvoir circuler anonymement.

46 Article 4 paragraphe (1) lettre (b) de la loi modifiée du 2 août 2002.

7

7. Types de surveillance

Le législateur a prévu des restrictions claires afin d'alléger le caractère intrusif des dispositifs de géolocalisation. Celles-ci sont notamment précisées dans les autorisations de la CNPD et découlent des principes généraux de la loi sur la protection des données.

7.5.3.1. Interdiction d'une surveillance permanente

Un système de géolocalisation ne peut pas être utilisé dans le but de contrôler de manière permanente les salariés sous peine d'être considéré comme une « filature » électronique qui porte nécessairement atteinte au respect de la vie privée des personnes concernées. Sauf pour des hypothèses très précises et restrictives, la loi prévoit seulement la surveillance du salarié de manière temporaire et, en plus, sous certaines conditions restrictives.

7.5.3.2. Interdiction de surveiller toutes les prestations des salariés

Les données recueillies par l'employeur ne pourront pas servir à observer les performances et/ou le comportement des salariés en dehors des finalités sur lesquelles est fondée l'autorisation de la CNPD.

En effet, le responsable du traitement ne doit pas perdre de vue que le but principal recherché par la surveillance est de pouvoir contrôler son infrastructure matérielle comprenant ses véhicules et les biens y entreposés et que la surveillance des prestations des salariés n'est donc qu'accessoire.

7.5.3.3. Interdiction de contrôler les salariés en dehors des heures de travail

Si le salarié est autorisé à utiliser le véhicule professionnel à des fins privées, c'est-à-dire en dehors des heures de travail, l'employeur doit nécessairement lui offrir la possibilité de désactiver le dispositif de géolocalisation. En aucune hypothèse, l'employeur n'a le droit de surveiller le salarié en dehors de ses heures de travail. Reste à noter que si le véhicule est exclusivement à usage professionnel, l'activation du système peut être permanente.

7.5.3.4. Interdiction de contrôler le respect des limitations de vitesse

L'employeur ne peut pas traiter les données relatives aux excès de vitesse. Cette interdiction est expressément mentionnée à l'article 8 paragraphe (2) de la loi modifiée du 2 août 2002 disposant que « *les traitements de données relatives aux infractions (...) ne peuvent être mis en œuvre qu'en exécution d'une disposition légale* ». Ne posent pas de problème les données suivantes : 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.

7.5.3.5. Durée de conservation limitée

Les données de localisation peuvent seulement être conservées pendant une période maximale de deux mois.

En cas d'incident, les données peuvent toutefois être conservées au-delà du délai prémentionné dans le cadre de la transmission des données aux autorités judiciaires compétentes pour constater ou pour poursuivre des infractions pénales.

Les données et paramètres purement techniques relatifs au véhicule peuvent être conservés au-delà d'une durée de deux mois à condition toutefois que les données à caractère personnel du traitement aient été préalablement effacées sinon rendues anonymes.

Pour finir, les données relatives au temps de travail peuvent être conservées pendant une durée maximale de trois ans conformément au délai de prescription posé à l'article 2277 alinéa 1er du Code Civil en matière d'action en paiement de rémunérations des salariés.

7.6. Surveillance des accès aux locaux et contrôle des horaires de travail

La surveillance des accès aux locaux ou le contrôle des horaires de travail par badge/carte ou code, permettant d'identifier directement ou indirectement le salarié détenteur, constituent des traitements de données à caractère personnel et sont donc soumis aux prescrits de la loi sur la protection des données.

Les systèmes de surveillance des accès sont destinés à la gestion et au contrôle des accès physiques à l'entrée de sites, bâtiments, locaux ou à certaines zones limitativement identifiées qui font l'objet d'une restriction de circulation.

Les systèmes de contrôle des horaires de travail, utilisés dans le cadre d'une organisation de travail selon l'horaire mobile ou des horaires fixes, sont destinés à la gestion et au contrôle des horaires de travail et des temps de présence sur le lieu de travail.

Dans un souci d'allègement des formalités à l'égard des employeurs, la CNPD a par ailleurs mis en place une autorisation unique pour ces traitements.

7.6.1. Quels peuvent être les objectifs poursuivis par l'employeur ?

Contrôle des accès aux locaux

Le traitement de données à caractère personnel relatif aux **travailleurs** ne peut être mis en œuvre que :

- pour les besoins de sécurité et de santé des travailleurs, sous réserve d'avoir obtenu préalablement l'accord du comité mixte, le cas échéant institué,
- pour les besoins de protection des biens de l'entreprise (dans ce cas l'accord du comité mixte n'est pas requis).

Le traitement de données portant sur les **tiers** ne pourra être effectué que :

- si la personne concernée a donné son consentement (au sens de la définition de l'article 2 lettre (c) de la loi du 2 août 2002), ou
- 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, ou
- aux lieux d'accès privé dont la personne physique ou morale y domiciliée ou établie est le responsable du traitement.

Contrôle des horaires de travail

Le traitement de données à caractère personnel relatif aux **travailleurs** ne peut être mis en œuvre que s'il est nécessaire dans le cadre d'une organisation de

7

7. Types de surveillance

travail selon l'horaire mobile conformément à la loi, sous réserve d'avoir obtenu préalablement l'accord du comité mixte, le cas échéant institué.

Sont donc visés tous les traitements de données effectués en vue du contrôle des horaires de présence des travailleurs, de leur identification à leur entrée et sortie, des plages obligatoires, de la vérification du respect des règles de compensation et de leur incidence sur la rémunération et la compensation des congés.

Se pose donc la question de savoir si l'employeur peut également procéder a une surveillance des temps de présence fixes, du fait que l'article L.261-1 paragraphe (1) point (5) fait expressément et exclusivement référence à une organisation du travail « selon l'horaire mobile conformément au présent code ».

À ce titre, la Commission nationale est d'avis que faire une distinction entre une organisation de travail selon l'horaire mobile et celle selon l'horaire fixe serait dénuée de tout fondement et contraire à l'organisation et au bon fonctionnement de l'entreprise. En outre, cette distinction reviendrait à interdire à l'employeur de mesurer par un moyen technique quelconque le temps de présence des salariés travaillant selon un horaire fixe, et d'en déduire le cas échéant le montant exact de la rémunération leur revenant au titre des heures effectivement prestées.

Partant du postulat que l'atteinte à la vie privée des salariés est strictement la même indépendamment du mode d'organisation de travail choisi par l'employeur (horaire mobile ou horaire fixe), qu'aux yeux du législateur ce type de surveillance n'est pas considéré comme excessif, la Commission nationale considère en l'occurrence que, nonobstant le libellé restrictif du critère de légitimation de l'article L.261-1 paragraphe (1) point (5), une telle surveillance peut être effectuée par l'employeur.

Pour ce qui est du contrôle des horaires de travail relatif à **des tiers**, il convient de relever que les mesures de surveillance des horaires de travail et des temps de présence sur le lieu de travail ne concernent en principe que les salariés du responsable du traitement. Il existe cependant des hypothèses où des tiers (p.ex. les employés d'un sous-traitant, fournisseur, etc.) effectuent des prestations au sein des locaux du responsable du traitement pendant une période plus ou moins longue et sont, à ce titre, soumis à une telle surveillance, notamment pour vérifier la conformité aux contrats de services souscrits par le responsable du traitement. Dans ces situations, la CNPD retient que la seule condition de légitimité susceptible de trouver application est le consentement exprès et non équivoque de l'intervenant externe.

7.6.2. L'autorisation préalable de la CNPD, assortie de conditions

Chaque fois qu'un salarié utilise un badge, une carte magnétique ou un code, le système enregistre des données le concernant. Ces enregistrements peuvent être utilisés pour « tracer » ses déplacements et présentent des risques de détournements de finalité.

Afin de minimiser ces risques, les conditions qui sont précisées dans les autorisations de la CNPD doivent être respectées par l'employeur.

Finalités du traitement

Le traitement mis en œuvre concernant la **surveillance des accès** ne doit servir que pour contrôler les entrées et sorties des sites, bâtiments et locaux de l'employeur. Il ne doit pas être détourné de sa finalité, c'est-à-dire qu'il ne doit pas être utilisé pour le contrôle des déplacements à l'intérieur du lieu de travail, à l'exception des cas dans lesquels certaines zones identifiées font l'objet d'une restriction de circulation justifiée par la sécurité des biens et des personnes qui y travaillent.

En ce qui concerne la **surveillance des horaires de travail**, les données collectées par l'employeur ne

peuvent être utilisées que pour gérer et vérifier les heures d'arrivée sur le lieu de travail et les heures de départ du lieu de travail.

Durée de conservation

Une durée limitée de conservation de données constitue une garantie supplémentaire pour éviter d'éventuels détournements de finalité.

Pour la surveillance des accès, les données ne doivent pas être conservées plus de trois mois à compter de leur enregistrement, à moins que le traitement porte en même temps sur le contrôle des horaires de travail (p.ex. si un seul badge est utilisé pour les deux finalités). Dans ce cas, les données personnelles des travailleurs salariés et assimilés ne doivent pas être conservées au-delà de trois ans[47].

Les données personnelles des agents publics ne doivent pas être conservées au-delà de cinq ans[48].

Dans l'hypothèse d'une contestation ou d'un incident, les données s'y rapportant ne font pas l'objet de l'obligation de destruction au bout des délais susmentionnés, si elles ont été transmises aux autorités compétentes.

7.6.3. Des formalités allégées

Les deux types de traitements analysés ci-avant sont soumis au régime de l'autorisation préalable de la CNPD. Consciente du fait qu'un nombre important d'employeurs utilisent ces dispositifs et soucieuse de faciliter les formalités administratives préalables à remplir par les responsables du traitement, la CNPD a mis en place une procédure d'autorisation allégée (autorisation unique[49]). Ceci n'est pas le cas pour les systèmes biométriques qui restent soumis à la procédure d'autorisation ordinaire[50].

Par une **décision unique**, la CNPD peut autoriser de manière générale certains traitements de données qui :

- ont une même finalité,
- portent sur des catégories de données identiques et
- ont les mêmes destinataires ou catégories de destinataires.

Pour pouvoir bénéficier d'une autorisation unique, le responsable du traitement doit adresser à la CNPD un **engagement formel** par lequel il déclare que le traitement est conforme à la description figurant dans la décision unique.

47 *Ce délai est conforme aux dispositions de l'article 2277 du Code Civil.*

48 *Cf.* ***Cour Admin., 11 juin 1998, n°10607C****.*

49 *Délibération n°63/2007 du 22 juin 2007 : Autorisation unique relative aux traitements de données à caractère personnel portant sur le contrôle des horaires de travail dans le cadre d'une organisation de travail selon l'horaire mobile. Délibération n°64/2007 du 22 juin 2007 : Autorisation unique relative aux traitements de données à caractère personnel portant sur la surveillance des accès.*

50 *Voir point 7.4.*

NOTIZEN / NOTES

dialogue

THÉMATIQUE

LA SURVEILLANCE SUR LE LIEU DE TRAVAIL

La présente publication a pour objet d'informer le lecteur sur les droits et obligations des salariés et des employeurs sur le lieu de travail en ce qui concerne le traitement des données à caractère personnel utilisées à des fins de surveillance ainsi que sur le rôle important que joue la Commission nationale pour la protection des données (CNPD) dans cette matière.

Dans un premier temps sont exposés les deux régimes applicables au traitement de données à caractère personnel à des fins de surveillance :

- les traitements à des fins de surveillance des tiers (régime général),
- les traitements à des fins de surveillance des salariés sur le lieu de travail (régime spécifique).

Dans un deuxième temps sont analysées les différentes formes de surveillance qui sont utilisées sur le lieu de travail telles que :

- la vidéosurveillance,
- le contrôle de l'utilisation des outils informatiques,
- l'enregistrement des conversations téléphoniques,
- les systèmes de reconnaissance biométrique,
- les dispositifs de géolocalisation et
- les systèmes de surveillance des accès et des horaires de travail.

Pour chaque forme de surveillance, les auteurs ont essayé, dans la mesure du possible, de donner des exemples concrets illustrés par des jurisprudences.

DIE ÜBERWACHUNG AM ARBEITSPLATZ

Die vorliegende Veröffentlichung zielt darauf ab, den Leser über die Rechte und Pflichten der Arbeitnehmer und Arbeitgeber im Bereich der Verarbeitung personenbezogener Daten zu Überwachungszwecken am Arbeitsplatz und über die diesbezügliche bedeutende Rolle der Nationalen Kommission für den Datenschutz (CNPD) zu informieren.

Zunächst werden die beiden Regelungen dargelegt, die auf die Verarbeitung personenbezogener Daten zu Überwachungszwecken Anwendung finden:

- Datenverarbeitung zur Überwachung Dritter (allgemeine Regelung),
- Datenverarbeitung zur Überwachung der Arbeitnehmer am Arbeitsplatz (Sonderregelung).

Danach werden die am Arbeitsplatz eingesetzten verschiedenen Formen der Überwachung analysiert, wie beispielsweise:

- die Videoüberwachung,
- die Kontrolle der Verwendung von IT-Tools,
- die Aufzeichnung von Telefongesprächen,
- die biometrischen Erkennungssysteme,
- die Geolokalisierungsgeräte,
- die Systeme zur Zutrittsüberwachung und zur Überwachung der Arbeitszeiten.

Die Autoren haben versucht, für jede Überwachungsform soweit möglich konkrete Beispiele zu nennen und diese anhand der Rechtsprechung zu veranschaulichen.

Diffusée par :

Librairie Um Fieldgen
3, rue Glesener - L-1631 Luxembourg
info@libuf.lu

Cette publication est également disponible au siège de la CSL.

Editée par :

CHAMBRE DES SALARIES
LUXEMBOURG

18 rue Auguste Lumière L-1950 Luxembourg
T +352 27 494 200 F +352 27 494 250
csl@csl.lu www.csl.lu

Prix : 4€

ISSN : 5-453002-011003