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.*

DIE ÜBERWACHUNG AM ARBEITSPLATZ

Impressum

Herausgeber

Arbeitnehmerkammer
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, Präsident
Norbert Tremuth, Direktor

Nationale Kommission für den Datenschutz
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, Präsident
Thierry Lallemang, ordentliches Mitglied
Pierre Weimerskirch, ordentliches Mitglied

Druck

Druckerei WePrint

Vertrieb

Buchhandlung „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

Vorwort

Es liegt auf der Hand, dass die neuen Informations- und Kommunikationstechnologien (NIKT) einen immer rasanteren Aufschwung erleben und immer stärkeren Einfluss auf die privaten und beruflichen Beziehungen der Bürger nehmen.

Obgleich der Austausch personenbezogener Daten somit zu einer Realität und Notwendigkeit für die Entwicklung der wirtschaftlichen Tätigkeiten unseres Landes geworden ist, muss man unweigerlich feststellen, dass diese Daten zunehmend auf unsere Privatsphäre übergreifen. Diese beunruhigende Entwicklung betrifft sowohl die Privatsphäre der Menschen als auch deren berufliches Umfeld.

Am Arbeitsplatz stehen sich die Interessen der Arbeitgeber in Bezug auf die Gewährleistung des reibungslosen Betriebs und der ordnungsgemäßen Entwicklung des Unternehmens und die Interessen der Arbeitnehmer in Bezug auf den Schutz ihrer Privatsphäre gegenüber und müssen demnach in ein ausgewogenes Gleichgewicht gebracht werden. Das Gesetz und die Rechtsprechung haben die hierfür anwendbaren Regeln aufgestellt. Das Recht der Arbeitnehmer auf den Schutz ihrer Privatsphäre am Arbeitsplatz wurde seitens der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte anerkannt.

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).

Jean-Claude REDING
Präsident der CSL

Gérard LOMMEL
Präsident der CNPD

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, jede Überwachungsform soweit möglich anhand von Fällen aus der Rechtsprechung zu veranschaulichen.

Die CSL und die CNPD hoffen, dass die vorliegende Broschüre den Leser über die Rechte und Pflichten des Arbeitnehmers und des Arbeitgebers im Bereich der Verarbeitung personenbezogener Daten zu Überwachungszwecken am Arbeitsplatz aufklären kann.

Luxemburg, Oktober 2014

Inhalt

Inhalt

1

1. Einleitung

Der Bereich der neuen Technologien entwickelt sich heutzutage in rasendem Tempo. Der Einsatz dieser neuen Technologien ist der Beginn einer tiefgreifenden und unabwendbaren Veränderung unserer gesamten Gesellschaft. Obgleich die Vorteile dieser Technologien unumstritten sind, muss man unweigerlich feststellen, dass sie uns gegenüber auch immer penetranter und aufdringlicher werden. Diese beunruhigende Entwicklung betrifft sowohl die Privatsphäre der Menschen als auch deren berufliches Umfeld.

Die Arbeitsumgebung bleibt von den jüngst erzielten Fortschritten im Technologiebereich nicht verschont. In einem Umfeld, in dem der Arbeitgeber versucht, sein Unternehmen wirksam und mit maximaler Rentabilität zu verwalten, möchte dieser natürlich auch die neuen Technologien für sich ausnutzen, mit der die Tätigkeit der Arbeitnehmer nun aber so detailliert verfolgt werden kann, wie es vor einigen Jahren noch undenkbar gewesen wäre.

Ob es sich nun um die jüngsten Entwicklungen in den Bereichen Geolokalisierung, Videoüberwachung oder Biometrie handelt, oder um IT-Systeme, die eine minuziöse Überwachung der Verwendung von IT-Tools ermöglichen - die unter Einsatz dieser neuen Technologien erfolgende Kontrolle der Tätigkeiten der Arbeitnehmer ist im Laufe der vergangenen Jahre wesentlich vielfältiger geworden. Die Entwicklung des BYOD-Konzepts („Bring Your Own Device") löst ebenfalls Streitfragen zwischen den Rechten und Interessen des Arbeitgebers und dem Schutz der Privatsphäre der Arbeitnehmer aus.

Diese Geräte zeichnen allesamt natürlich auch zahlreiche personenbezogene Daten über die Arbeitnehmer auf. Ihr Einsatz könnte infolgedessen die Rechte der Arbeitnehmer und den Schutz der Privatsphäre der Arbeitnehmer am Arbeitsplatz stark gefährden, bei dem es sich um ein in der europäischen Rechtsprechung verankertes Recht handelt: *„Es scheint darüber hinaus kein prinzipieller Grund zu bestehen, warum diese Auffassung von „Privatleben" die Tätigkeiten beruflicher oder geschäftlicher Natur ausschließen sollte, da schließlich im Verlauf ihres Arbeitslebens die Mehrzahl der Menschen eine signifikante, wenn nicht die größte Chance haben, Beziehungen zur Außenwelt aufzunehmen"*, **EGMR, Niemietz gegen Deutschland, 16. Dezember 1992. Vgl. diesbezüglich: EGMR, Halford gegen Vereinigtes Königreich, 27. Juli 1997; EGMR, Copland gegen Vereinigtes Königreich, 3. April 2007; EGMR, Peev gegen Bulgarien, 26. Juli 2007**.

Um jedweder potenziellen Abdrift entgegenzuwirken, hat der luxemburgische Gesetzgeber eine besondere rechtliche Regelung für die Datenverarbeitung zu Überwachungszwecken eingerichtet, die in gewisser Weise in einer Abwägung der unterschiedlichen Interessen besteht, die zum einen für den Arbeitgeber im Recht auf die Überwachung des ordnungsgemäßen Betriebs seines Unternehmens und zum anderen für die Arbeitnehmer im Recht auf den Schutz ihrer Privatsphäre am Arbeitsplatz liegen.

Wie können diese beiderseitigen Rechte bei der Einrichtung einer Überwachung am Arbeitsplatz in Einklang gebracht werden? Welche gesetzlichen Bestimmungen sind einzuhalten? Aus welchen Gründen könnte ein Arbeitgeber zur Einrichtung von Überwachungsmaßnahmen bewogen werden? Welche Maßnahmen müssen die Arbeitgeber zur Einhaltung der Gesetze ergreifen? Welche Rechte haben die Arbeitnehmer? Wie sind sie geschützt?

Die vorliegende Broschüre möchte Antworten auf alle diese Fragen liefern.

2. Der Begriff „Überwachung“

Durch das abgeänderte Gesetz vom 2. August 2002 zum Schutz personenbezogener Daten bei der Datenverarbeitung (nachstehend: „das abgeänderte Gesetz vom 2. August 2002“ oder „das Gesetz“) wird die europäische Richtlinie 95/46/EG des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr in nationales Recht umgesetzt.

An dieser Stelle sei anzumerken, dass die besagte Richtlinie keine spezifischen Bestimmungen in Bezug auf die Überwachung enthält. Aus Sorge um die Rechte der Arbeitnehmer und Bürger, und in Anbetracht dessen, dass die Richtlinie kein diesbezügliches Verbot enthält, wollte der Luxemburger Gesetzgeber dieses Thema durch ein Gesetz regeln. Letzteres definiert die „Überwachung“ wie folgt:

„Jede Aktivität, die mittels Einsatz technischer Mittel in der regelmäßigen Beobachtung, Erhebung oder Aufzeichnung von personenbezogenen Daten einer oder mehrerer Personen in Bezug auf Verhaltensweisen, Bewegungen, Kommunikationen oder in Bezug auf die Verwendung von elektronischen oder computergesteuerten Geräten besteht.“[1]

Aus dieser sehr weit gefassten gesetzlichen Definition lässt sich ableiten, dass der Begriff der Überwachung sehr unterschiedliche Formen der Überwachung umfasst, wie beispielsweise:

- die Videoüberwachung,
- die Kontrolle der Verwendung von IT-Tools (beispielsweise Logs der im Internet besuchten Seiten, Überprüfung der versandten und empfangenen E-Mails, Verwendung des betriebsinternen Netzwerks, usw.),
- die Aufzeichnung von Telefongesprächen,
- die biometrischen Erkennungssysteme,
- die Geolokalisierungsgeräte,
- die Systeme zur Zutrittsüberwachung und zur Überwachung der Arbeitszeiten.

Bevor wir diese verschiedenen Überwachungsarten und deren Besonderheiten genauer untersuchen, empfiehlt sich zunächst die Analyse der spezifischen Bestimmungen in Bezug auf die Überwachung, um danach die auf die Überwachung am Arbeitsplatz anzuwendenden Grundsätze genauer zu untersuchen.

1 *Artikel 2 (p) des abgeänderten Gesetzes vom 2. August 2002.*

3

3. Die luxemburgische Gesetzgebung

Im Bemühen um den Schutz der Personen, hat der Luxemburger Gesetzgeber einen ziemlich restriktiven Rechtsrahmen in Bezug auf die Datenverarbeitung zu Überwachungszwecken geschaffen. Eine der Hauptzielsetzungen des Gesetzgebers bestand dabei darin, bei der Einrichtung dieser spezifischen Regelung für die Überwachung[2], die sich von den in unseren Nachbarländern eingesetzten Regelungen dahingehend unterscheidet, dass sie größtenteils restriktiver ist, das Phänomen des *„Big brother is watching you"* zu vermeiden. Durch diesen restriktiven Ansatz kann ein bedeutendes Maß an Rechtssicherheit unter gleichzeitiger Minimierung der Konflikte zwischen den betreffenden Interessen gewährleistet werden.

Im abgeänderten Gesetz vom 2. August 2002 werden alle Fälle aufgezählt, in denen eine Überwachung stattfinden kann, wobei klar zwischen zwei Regelungen zu unterscheiden ist:

- Datenverarbeitung zur **Überwachung Dritter** (Artikel 10 des Gesetzes) (allgemeine Regelung)
- Datenverarbeitung zur **Überwachung der Arbeitnehmer am Arbeitsplatz** (früherer Artikel 11, ersetzt durch Artikel 11 neu[3]).

Der neue Artikel 11 findet auf die Verarbeitung personenbezogener Daten zum Zwecke der seitens des Arbeitgebers erfolgenden Überwachung seiner Arbeitnehmer Anwendung. Er verweist auf die in Artikel L.261-1 des Arbeitsgesetzbuches aufgezählten spezifischen Bedingungen. Damit diese Regelung Anwendung findet, muss ein rechtliches **Unterordnungsverhältnis** zwischen dem für die Verarbeitung Verantwortlichen und der von der Überwachung betroffenen Person vorliegen.

Bei Zweifeln über das Vorliegen eines rechtlichen Unterordnungsverhältnisses genügt es, sich auf die seitens der nationalen Rechtsprechung diesbezüglich ausgearbeiteten Kriterien zu beziehen[4]. Überdies ist anzumerken, dass den „Arbeitnehmern" im Rahmen des neuen Artikels 11 auch Beamte und Angestellte des öffentlichen Dienstes sowie Zeitarbeitskräfte gleichgestellt sind, nicht jedoch Arbeitnehmer externer Dienstleister.

Die in Artikel 10 enthaltene Regelung stellt die allgemeine Regelung dar, die auf alle Situationen außerhalb des Beschäftigungsbereichs Anwendung findet. Dieser Artikel gilt demnach für alle vom neuen Artikel 11 nicht abgedeckten Fälle. Folglich findet er auf die Datenverarbeitung zum Zwecke der Überwachung Dritter seitens eines für die Verarbeitung Verantwortlichen Anwendung. Unter Dritten sind alle Personen zu verstehen, bei denen es sich nicht um die Arbeitnehmer des für die Verarbeitung Verantwortlichen handelt, d.h. alle Personen, die keinem oben genannten rechtlichen Unterordnungsverhältnis unterstehen. Am Arbeitsplatz sind unter Dritten demnach beispielsweise die Kunden, die Besucher, die Lieferanten, die externen Berater, usw. zu verstehen.

Je nach eingesetztem Überwachungsmittel kann es sein, dass ein und dieselbe Datenverarbeitung in Abhängigkeit von der betroffenen Person (Dritter oder Arbeitnehmer) in den Anwendungsbereich von Artikel 10 und 11 fällt.

2 *Siehe Parlamentsdokument Nr. 4735/00, S. 36.*

3 *Siehe Art. 10 des Gesetzes vom 27. Juli 2007 zur Änderung des Gesetzes vom 2. August 2002.*

4 *„Damit ein rechtliches Unterordnungsverhältnis vorliegt, muss der Vertrag den Arbeitnehmer seinem Arbeitgeber unterstellen, der ihm Anweisungen in Bezug auf die Arbeitsleistung erteilt, deren Durchführung kontrolliert und deren Ergebnisse überprüft", siehe* ***Gerichtshof 1. Februar 1978, Scheidtweiler gegen Express SA; Gerichtshof 21. Dezember 1989, Gillain gegen Flebus und Laroire; Gerichtshof 14. Mai 1993, Wassermann gegen Transcomerz; Gerichtshof 9. Januar 1997, Parravano gegen Winlux SA****, zitiert in: Le Contrat de Travail - Droit et Jurisprudence, R. Schintgen und J. Faber, Veröffentlichung des Ministeriums für Arbeit und Beschäftigung, Januar 2010, S. 16.*

Daher ist die Überwachung Dritter in der vorliegenden Broschüre ebenfalls kurz anzusprechen. Insbesondere im Bereich der Videoüberwachung finden beide Regelungen sehr häufig gemeinsam Anwendung, sofern auch Personen von der Überwachung betroffen sind, bei denen es sich nicht um Arbeitnehmer des für die Verarbeitung Verantwortlichen handelt. Dies gilt beispielsweise für den Fall einer Supermarkt-Kamera, die sowohl die Arbeitnehmer des Geschäfts (neuer Artikel 11) als auch Dritte (Kunden, Artikel 10) filmt. In gleicher Weise kann die Aufzeichnung von Telefongesprächen seitens einer Bank sowohl die Arbeitnehmer (neuer Artikel 11) als auch die Kunden (Artikel 10) betreffen.

4

4. Welche Zielsetzungen kann der Arbeitgeber verfolgen? Die Zweckbestimmung als Schlüsselbegriff jeder Datenverarbeitung.

Mit jeder Datenverarbeitung wird von Haus aus eine bestimmte Zielsetzung verfolgt. Die klare und genaue Festsetzung dieser Zielsetzung ermöglicht nicht nur die konkrete Bestimmung der zur Erreichung dieser Zielsetzung durchzuführenden Maßnahmen, sondern auch die Absteckung deren genauen Grenzen[5].

Die Bestimmung des oder der zu erzielenden Zwecke ist eine erforderliche Voraussetzung für die Anwendung und Bewertung der übrigen untrennbar damit verbundenen Kriterien. Zu diesen Kriterien zählt, dass die Daten für **festgelegte, eindeutige und zulässige** Zwecke erhoben und nicht auf mit diesen Zweckbestimmungen unvereinbare Weise weiterverarbeitet werden[6]. Der Grundsatz der Umgrenzung der Zweckbestimmung bestimmt folglich, in welchem Umfang die persönlichen Daten erfasst, verarbeitet und weiterverwendet werden dürfen oder nicht. Dieser Schlüsselgrundsatz ermöglicht den Schutz der betroffenen Person durch die Begrenzung der Verwendungsart der Daten seitens des für die Verarbeitung Verantwortlichen und trägt demnach zur größeren Transparenz, Rechtssicherheit und Vorhersehbarkeit einer Verarbeitung personenbezogener Daten bei.

Bei dem **für die Verarbeitung Verantwortlichen** handelt es sich um *„die natürliche oder juristische Person, die öffentliche Behörde, die Dienststelle oder jede andere Einrichtung, die allein oder gemeinsam mit anderen die Zweckbestimmungen und die Mittel für die Verarbeitung personenbezogener Daten festlegt"*[7].

5 *Siehe Parlamentsdokument Nr. 4735/00, S. 30 f.*

6 *Artikel 4, Absatz (1), Buchstabe (a) des Gesetzes.*

7 *Artikel 2, Buchstabe (n) des Gesetzes.*

Unter **festgelegtem Zweck** ist demnach ein Zweck zu verstehen, der derart genau definiert ist, dass er eine klare und genaue Umgrenzung des Anwendungsbereichs der Verarbeitung ermöglicht.

Um als **eindeutig** betrachtet zu werden, muss der Zweck hinreichend klar und unzweideutig zum Ausdruck gebracht werden (kein versteckter Zweck).

Die **Zulässigkeit** erfordert, dass sich der für die Verarbeitung Verantwortliche ausschließlich auf die vom Gesetz vollständig festgesetzten Zulässigkeitskriterien stützen darf. Im Rahmen einer Überwachung gelten die in Artikel 5 des Gesetzes dargelegten allgemeinen Zulässigkeitskriterien jedoch nicht. Artikel 10 (Überwachung Dritter) und der neue Artikel 11 (Überwachung am Arbeitsplatz) weichen von den in Artikel 5 des Gesetzes dargelegten allgemeinen Zulässigkeitsbedingungen ab. Folglich sind die Vorbedingungen einer Überwachung, d.h. die einzig anerkannten Zielsetzungen, aus denen eine Überwachung durchgeführt werden kann, in diesen beiden Artikeln dargelegt[8]. Eine genaue Untersuchung dieser Vorbedingungen, die in Abhängigkeit von der Art der Überwachung variieren, erfolgt in den Punkten 5.1. und folgende der vorliegenden Broschüre.

Die genaue Bestimmung des Zwecks ist auch entscheidend, um zu vermeiden, dass dieser nicht entfremdet wird. Ein Beispiel einer solchen Zweckentfremdung wäre die Verwendung von Bildern aus einem Videoüberwachungssystem, das zum Schutz des Zutritts

8 *Seitens der Rechtsprechung bestätigte Position, siehe insbesondere Verwaltungsgericht Luxemburg,* ***15. Dezember 2004, Nr. 17890****, bestätigt seitens des Verwaltungsgerichtshofs Luxemburg, 12. Juli 2005,* ***Nr. 19234 C****; siehe auch Verwaltungsgericht Luxemburg,* ***9. Mai 2005, Nr. 18680; Verwaltungsgericht Luxemburg, 21. Mai 2007, Nr. 22050****.*

zum Gebäude des für die Verarbeitung Verantwortlichen eingerichtet wurde, seitens des Arbeitgebers jedoch zur Überprüfung der Anwesenheitszeiten seiner Arbeitnehmer eingesetzt wird. Eine Zweckentfremdung wäre auch ein Videoüberwachungssystem für eine Fertigungslinie, das ausschließlich auf die Maschinen abzielt, dessen Bilder jedoch beispielsweise zur Überwachung des Verhaltens oder der Leistung einer oder mehrerer Arbeitnehmer verwendet werden.

Aus Vorstehendem geht hervor, dass die Zwecke, aus denen ein für die Verarbeitung Verantwortlicher seine Arbeitnehmer überwacht, in Abhängigkeit von der Art der eingesetzten Überwachung variieren. Da die Überwachung eine besondere Gefahr für die Privatsphäre der Arbeitnehmer darstellt, hat sich der Gesetzgeber zum Schutz der von den Überwachungsmaßnahmen betroffenen Personen für die Regelung der Vorabgenehmigung entschieden. Diesbezüglich verfügt die Nationale Kommission für den Datenschutz (nachstehend „die Nationale Kommission" oder „die CNPD") vor der Erteilung einer Genehmigung zur Überwachung über eine Ermessensbefugnis bei der Analyse der **Notwendigkeit** und **Verhältnismäßigkeit**[9] der seitens des Arbeitgebers geplanten Überwachungsmaßnahmen.

So kann beispielsweise eine über ein Geolokalisierungssystem erfolgende Überwachung der Fahrzeuge eines Unternehmens als notwendig und verhältnismäßig betrachtet werden, sofern der Arbeitnehmer über das Fahrzeug lediglich indirekt überwacht wird. Wenn das Geolokalisierungsgerät hingegen am Körper des Arbeitnehmers getragen wird, ist die Nationale Kommission außer in sehr seltenen Ausnahmefällen der Ansicht, dass das Überwachungsmittel unverhältnismäßig ist, da es dem Arbeitgeber die sekunden- und metergenaue Überwachung der Fortbewegung des Arbeitnehmers selbst ermöglicht.

Die Bestimmung der Zwecke einer seitens des Arbeitgebers erfolgenden Verarbeitung stellt demnach zweifelsohne einen entscheidenden Faktor im Hinblick darauf dar, ob ihm eine entsprechende Genehmigung erteilt wird oder nicht.

9 *Seitens der Rechtsprechung bestätigt, siehe insbesondere Verwaltungsgericht Luxemburg,* ***15. Dezember 2004, Nr. 17890****, bestätigt seitens des Verwaltungsgerichtshofs Luxemburg,* ***12. Juli 2005, Nr. 19234 C****; siehe auch Verwaltungsgericht Luxemburg,* ***21. Mai 2007, Nr. 22050****.*

5

5. Wie sind die Arbeitnehmer geschützt?

Das abgeänderte Gesetz vom 2. August 2002 gewährleistet den von einer Überwachungsmaßnahme betroffenen Arbeitnehmern und Dritten (nicht beim jeweiligen Arbeitgeber angestellte Personen) einen verschärften Schutz. Die Gewährleistung dieses Schutzes erfolgt insbesondere durch:

- einen eng begrenzten und detaillierten Katalog der Vorbedingungen, die eine Überwachung ermöglichen (**Kapitel 5.1**);
- die von Fall zu Fall erfolgende Vorabuntersuchung seitens der CNPD, deren Genehmigung einerseits das Recht der Arbeitnehmer auf den Schutz ihrer Privatsphäre am Arbeitsplatz und andererseits das berechtigte Interesse des Arbeitgebers an der Einrichtung eines Überwachungssystems berücksichtigt (Analyse der Notwendigkeit und der Verhältnismäßigkeit der geplanten Überwachungsmaßnahmen/Abwägung der betreffenden Interessen) (**Kapitel 5.2**);
- die Einhaltung einer bestimmten Anzahl von Verpflichtungen seitens des für die Verarbeitung Verantwortlichen (**Kapitel 5.3**).

5.1. Die Fälle, in denen eine Überwachung möglich ist, sind gesetzlich begrenzt

5.1.1. Überwachung seitens des Arbeitgebers am Arbeitsplatz

Der neue Artikel 11 (der auf Artikel L.261-1 des Arbeitsgesetzbuches verweist) ermöglicht dem Arbeitgeber unter gewissen Bedingungen, seine Arbeitnehmer am Arbeitsplatz zu überwachen. Die Vorbedingungen, die eine solche Überwachung ermöglichen, wurden seitens des Gesetzgebers vollständig aufgezählt, d.h. eine Datenverarbeitung ist obligatorisch dadurch zu rechtfertigen, dass man sich auf eine der fünf gesetzlich vorgesehenen Zulässigkeitsbedingungen stützt. Keine andere (im Gesetz nicht genannte) Bedingung wird akzeptiert. Die Nationale Kommission ist der Ansicht, dass diese gesetzliche Bestimmung wörtlich zu verstehen und restriktiv auszulegen ist, da der Gesetzgeber eine erschöpfende Liste der ausdrücklichen Zulässigkeitsbedingungen erlassen hat, auf die er die Fälle der erlaubten Überwachung zu beschränken beabsichtigte.

Artikel L.261-1 des Arbeitsgesetzbuchs bestimmt, dass *„eine Verarbeitung nur dann erlaubt ist, wenn sie erforderlich ist:*

1. *für die Sicherheit und Gesundheit der Arbeitnehmer, oder*
2. *zum Schutz der Unternehmensgüter, oder*
3. *zur Kontrolle des Produktionsablaufs (ausschließlich auf Maschinenseite), oder*
4. *für die zeitweilige Kontrolle der Produktion oder der Leistungen des Arbeitnehmers, sofern eine derartige Maßnahme das einzige Mittel zur Festlegung der genauen Bezahlung ist, oder*
5. *im Rahmen der Arbeitsorganisation auf Basis von Gleitzeit nach Maßgabe des Arbeitsgesetzbuchs."*

Punkt 1 von Artikel L.261-1 kann seitens eines Arbeitgebers geltend gemacht werden, wenn die Tätigkeit seiner Arbeitnehmer je nach den Umständen derart beschaffen ist, dass sie eine potenzielle Gefährdung ihrer Sicherheit oder Gesundheit darstellt (was insbesondere eine Gefährdung ihrer körperlichen Unversehrtheit einschließen kann), oder weil die seitens der Arbeitnehmer ausgeübten Aufgaben gefährlich sind (gefährliche Maschinen, Vorhandensein von Giftstoffen), oder weil die Arbeitnehmer körperlichen Angriffen zum Opfer fallen könnten.

Dies trifft beispielsweise auf Geld- und Werttransportunternehmen zu, die ein Geolokalisierungssystem einsetzen. Aufgrund des Wertes der von ihnen in Gewahrsam genommenen Güter, können die Arbeitnehmer eines derartigen Unternehmens möglicherweise körperlichen Angriffen zum Opfer fallen – die Überwachungsmaßnahme mittels Geolokalisierung wäre demnach als zulässig zu betrachten, sofern sich der Verantwortliche für die Verarbeitung auf diese Vorbedingung stützt. Ein weiteres Beispiel ist die Videoüberwachung an einer Tankstelle, in einem Schmuckgeschäft oder in einer Bank. Eine derartige Überwachungsmaßnahme kann im Falle eines Raubüberfalls, eines Bankraubs oder selbst einer Geiselnahme zur Verhinderung der Gefährdung der körperlichen Unversehrtheit der Arbeitnehmer beitragen.

Punkt 2 von Artikel L.261-1 kann geltend gemacht werden, um eine Überwachung zur Verhinderung von Diebstählen oder Vandalismus zu rechtfertigen. Der **Begriff des Schutzes der Unternehmensgüter** umfasst sowohl die materiellen Güter (d.h. die beweglichen und unbeweglichen Güter) als auch die immateriellen Güter (Rechte des geistigen Eigentums, Geschäftsgeheimnisse, Forderungsbestände, usw.). Nach Ansicht der CNPD sollte der Begriff jedoch nicht den Schutz anderer als der in Verbindung mit klar identifizierbaren materiellen Gütern stehenden wirtschaftlichen Interessen des Unternehmens umfassen. Die Geltendmachung der Gefahr finanzieller Schäden, ungerechtfertigter Kosten oder entgangener Gewinne ist als Rechtfertigung unzureichend.

Dieses in Artikel L.261-1 enthaltene Zulässigkeitskriterium kann beispielsweise seitens eines Händlers geltend gemacht werden, der sein Warenlager überwachen möchte, um es vor Diebstahl zu schützen.

Der in Artikel L.261-1 dargelegte dritte Fall ist weniger verbreitet als die beiden ersten Fälle und zielt auf die rein beiläufige Überwachung der Arbeitnehmer im Zuge der hauptsächlichen Überwachung eines mechanischen Produktionssystems ab, wie beispielsweise eines automatisierten Bands zum Zusammenbau elektronischer Schaltkreise. Folglich zielt die Überwachung in erster Linie auf die Maschinen ab und die Arbeitnehmer könnten lediglich zweitrangig und zufällig überwacht werden. Im Fall der Videoüberwachung könnte es sich beispielsweise um einen Techniker handeln, der an einer Maschine der Fertigungslinie Reparaturarbeiten vornehmen muss und während dieser Zeit von Kameras gefilmt wird. Das Hauptziel dieser Kameras besteht nicht in der Überwachung des Technikers sondern beispielsweise in der Feststellung eines Produktionsfehlers oder einer Unterbrechung der Fertigungslinien. In diesem Fall ist die Überwachung der Arbeitnehmer zweitrangig und das mit der Überwachung verfolgte Hauptziel besteht in der Kontrolle der materiellen Infrastruktur, der Maschinen und der Werkzeuge, die der Arbeitgeber im Rahmen seiner beruflichen Tätigkeit besitzt.

Punkt 4. ist sehr selten, um nicht zu sagen in der Praxis nahezu unanwendbar. Die Unanwendbarkeit dieses Falls ergibt sich aus der seitens des Gesetzgebers vorgegebenen Auflage, dass die nachstehenden drei Bedingungen gleichzeitig erfüllt sein müssen: (i) es muss sich um eine zeitweilige Kontrolle handeln und die Überwachung muss zeitlich streng begrenzt sein; (ii) die Kontrolle darf sich nur auf die Produktion oder die Leistungen des Arbeitnehmers beziehen; und (iii) diese Maßnahme muss das einzige Mittel zur Festlegung der genauen Bezahlung darstellen. Zur Veranschaulichung wird auf Punkt 7.1.2.1. verwiesen.

Punkt 5. kann seitens eines Arbeitgebers geltend gemacht werden, der die Arbeits- und Anwesenheitszeiten seiner Arbeitnehmer am Arbeitsplatz kontrollieren möchte.

5

5. Wie sind die Arbeitnehmer geschützt?

5.1.1.1. Besondere Rolle des gemischten Betriebsrats

In den in den Punkten 1, 4 und 5 von Artikel L.261-1 des Arbeitsgesetzbuchs vorgesehenen Fällen, hat der gemischte Betriebsrat (sofern vorhanden) die in Artikel L.423-1, Punkte 1 und 2 des Arbeitsgesetzbuchs definierte **Entscheidungsbefugnis**. Den Parlamentsdokumenten zufolge, *„muss das oberste Ziel des Eingriffs des gemischten Betriebsrats darin bestehen, sicherzustellen, dass bei der Umsetzung des Überwachungsverfahrens die Grundsätze der Verhältnismäßigkeit und der Funktionalität in jedem Fall eingehalten werden*[10] *"*.

In diesen drei Fällen ist vor der Einreichung des Genehmigungsantrags folglich die Zustimmung des gemischten Betriebsrats einzuholen und der bei der CNPD einzureichenden Antragsakte beizufügen. Die Entscheidung des gemischten Betriebsrats stellt demnach in gewisser Weise einen ersten Filter im Rahmen des Ermessens der Umsetzung der Überwachung dar. Die Zweckbestimmungen der beiden anderen Vorbedingungen (Schutz der Unternehmensgüter und Kontrolle des Produktionsablaufs (ausschließlich auf Maschinenseite)) *„fallen nicht in den Zuständigkeitsbereich des gemischten Betriebsrats*[11] *"* und *„.... obliegen der Zuständigkeit des Arbeitgebers, der die Entscheidungsbefugnis in Bezug auf die Unternehmensorganisation behalten muss*[12] *"*.

Sollte das betreffende Unternehmen keinen gemischten Betriebsrat eingerichtet haben, ist die Zustimmung der Personalvertretung nicht erforderlich oder verpflichtend. Der Arbeitgeber ist jedoch in jedem Fall dazu verpflichtet, die Personalvertretungsorgane über die Durchführung einer Datenverarbeitung zu Überwachungszwecken in Kenntnis zu setzen[13] (siehe auch Punkt 5.3.1.).

10 *Parlamentsdokument Nr. 4735/07, S. 4.*

11 *Parlamentsdokument Nr. 4735/13, S. 21.*

12 *Ebenda.*

13 *Art. L.261-1, Para. (2) des Arbeitsgesetzbuchs*

Es ist jedoch anzumerken, dass die Bedeutung der Entscheidungsbefugnis des gemischten Betriebsrats durch eine Rechtsprechung des **Berufungsgerichts vom 26. Januar 2006**[14] relativiert wurde, die diesbezüglich feststellt, das die Nichtanrufung des gemischten Betriebsrats keinerlei Auswirkungen auf den Ausgang des Rechtsstreits hat, obgleich *„die Personalvertretung festgestellt hatte, dass das System Lücken aufwies"*.

5.1.1.2. Ausschluss der Einwilligung der Arbeitnehmer als Zulässigkeitskriterium

Das Gesetz sieht ausdrücklich vor, dass die Einwilligung des Arbeitnehmers als Zulässigkeitsfall der Überwachung am Arbeitsplatz ausgeschlossen wird. Der Arbeitgeber kann folglich von seinen Arbeitnehmer nicht die Unterzeichnung einer Einwilligungserklärung verlangen, durch die die seitens des Arbeitgebers geplanten Überwachungsmaßnahmen zulässig würden.

Dieser gesetzlich vorgesehene Ausschluss ist zum Schutz des Arbeitnehmers erforderlich, der sich in Bezug auf seinen Chef in einer untergeordneten Position befindet[15]. Sofern Letzterer von Rechts wegen die Einwilligung seines Arbeitnehmers verwenden könnte, könnte er diese beispielsweise immer in den Arbeitsvertrag einfügen und auf diese Weise die automatische Zustimmung des Arbeitnehmers zu den Überwachungsmaßnahmen auferlegen. Der Grundsatz des Schutzes der Privatsphäre des Arbeitnehmers am Arbeitsplatz würde dadurch beträchtlich geschwächt, um nicht zu sagen unterbunden werden.

14 ***Berufungsgericht Luxemburg, 26. Januar 2010, Nr.29384.***

15 *Siehe die obigen Ausführungen in Bezug auf das rechtliche Unterordnungsverhältnis.*

5.1.2. Überwachung von Personen, bei denen es sich nicht um Arbeitnehmer handelt („Dritte“)

Im Kapitel über die luxemburgische Gesetzgebung (Punkt 3, Seite 62) haben wir erfahren, dass es sein kann, dass ein und dieselbe Verarbeitung in Abhängigkeit von der betroffenen Person (Dritter oder Arbeitnehmer) in den Anwendungsbereich von Artikel 10 und Artikel 11 fallen kann. Je nach den jeweiligen Umständen können diese beiden Regelungen demnach gemeinsam Anwendung finden. Der am häufigsten anzutreffende Fall betrifft den Bereich der Videoüberwachung, in deren Rahmen Personen, bei denen es sich nicht um Arbeitnehmer des für die Verarbeitung Verantwortlichen handelt, ebenfalls von den Überwachungsmaßnahmen betroffen sind. Daher bietet es sich an dieser Stelle an, einige grundlegende Erklärungen in Bezug auf die Anwendung der allgemeinen Regelung von Artikel 10 zu liefern.

Die Bedingungen für die Überwachung von Personen, bei denen es sich nicht um Arbeitnehmer handelt, sind in Artikel 10 des abgeänderten Gesetzes vom 2. August 2002 aufgezählt. In diesem Fall erfolgt die Überwachung außerhalb jedes rechtlichen Unterordnungsverhältnisses[16] zwischen dem für die Verarbeitung Verantwortlichen und der überwachten Person.

In diesem Artikel heißt es, dass *„die Verarbeitung zu Überwachungszwecken nur vorgenommen werden kann:*

(a) *Wenn die betroffene Person ihre Einwilligung erteilt hat, oder*

(b) *In der unmittelbaren Umgebung oder an jedem anderen öffentlich zugänglichen oder nicht zugänglichen Ort außer in Wohnräumen, insbesondere in Parkhäusern, Bahnhöfen, Flughäfen und in den öffentlichen Transportmitteln, vorausgesetzt, dass der jeweilige Ort durch seine Art, seine Lage, seine Beschaffenheit oder seine Nutzung ein Risiko darstellt, das die Datenverarbeitung erforderlich macht:*

- *für die Sicherheit der Benutzer sowie für die Unfallverhütung; (...)*
- *für den Schutz der Güter, wenn ein ausgeprägtes Diebstahls- oder Vandalismusrisiko besteht, oder*

(c) *An den privaten Zutrittsorten, an denen die dort niedergelassene natürliche oder juristische Person der für die Verarbeitung Verantwortliche ist, oder*

(d) *Wenn die Verarbeitung zur Wahrung lebensnotwendiger Interessen der betroffenen Person oder einer anderen Person erforderlich ist, falls die betroffene Person aus physischen oder rechtlichen Gründen außer Stande ist, ihre Einwilligung zu erteilen.“*

Die erste Vorbedingung sieht vor, dass der für die Verarbeitung Verantwortliche die Einwilligung der betroffenen Person („bei der es sich nicht um einen Arbeitnehmer handelt“) einholen kann, um die Überwachung zulässig zu machen. Unter **Einwilligung** ist Nachstehendes zu verstehen: *„Jede freie, spezifische und in Kenntnis der Sachlage abgegebene Willensbekundung, durch welche die betroffene Person oder ihr gesetzlicher, rechtlicher oder satzungsgemäßer Vertreter einwilligt, dass die personenbezogenen Daten verarbeitet werden*[17]*“.*

Das Gesetz fordert zwar keine Schriftform, doch wird diese trotzdem empfohlen, damit der für die Verarbeitung Verantwortliche bei Bedarf den entsprechenden konkreten Nachweis erbringen kann. Die Einwilligung

16 Siehe obige Fußnote Nr. 4 zu Punkt 3. Seite 62.

17 Artikel 2, Buchstabe (c) des abgeänderten Gesetzes vom 2. August 2002.

5

5. Wie sind die Arbeitnehmer geschützt?

ist dennoch nicht passend oder geeignet, um in allen Situationen geltend gemacht zu werden. Das beste Beispiel dafür ist wahrscheinlich die Unmöglichkeit, sämtliche einer Videoüberwachungsmaßnahme unterliegenden Dritte um deren Einwilligung zu bitten, d.h. jedwede Person, die in das Sichtfeld einer Kamera gerät. In der Praxis kann die Einwilligung lediglich in bestimmten Fällen Anwendung finden.

Überdies ist noch festzustellen, dass selbst wenn die Einwilligung seitens eines für die Verarbeitung Verantwortlichen als Zulässigkeitskriterium geltend gemacht werden kann, die CNPD aus Gründen der Verhältnismäßigkeit eine Überwachung nach wie vor ablehnen kann. Dies kann beispielsweise bei bestimmten Arten der Verarbeitung biometrischer Daten der Fall sein.

Hierzu ist zu sagen, dass Punkt (b) im Hinblick auf eine Überwachung über Videokameras verfasst wurde und Orte (mit Ausnahme von Wohnräumen) betrifft, die die Überwachung aufgrund ihrer besonderen Merkmale für die Sicherheit der Benutzer oder für den Schutz der Güter erforderlich machen. Punkt (b) ist demnach **für andere Überwachungsarten kaum geeignet**.

Der in Artikel 10 (1) (c) genannte Begriff des *„Zutrittsortes"* wurde im Gesetz nicht definiert. Gemäß der Auslegung der CNPD, ist der Begriff des Zutrittsortes wie folgt zu verstehen: *„Die Stelle, über die man einen privaten Ort erreicht, unabhängig davon, ob es sich dabei um einen öffentlich zugänglichen oder öffentlich nicht zugänglichen Ort handelt"*. Dieser Punkt (c) ermöglicht insbesondere die Rechtfertigung einer Verarbeitung zum Zwecke der Überwachung Dritter, wenn diese die Räume eines Gebäudes betreten, ungeachtet dessen, ob es sich dabei um externe oder interne Zugänge handelt. Dabei kann es sich beispielsweise um Kunden eines Geschäfts handeln, die beim Überschreiten der Schwelle der Eingangstür gefilmt werden.

Die letzte Vorbedingung (Punkt (d)) kommt in der Praxis sehr selten vor. Sie kann beispielsweise auf eine Person Anwendung finden, die sich nach einer Operation in einem Aufwachraum befindet und deren kritischer Gesundheitszustand eine ständige Kameraüberwachung erfordert, um dem medizinischen Personal beim Auftreten von Komplikationen ein unverzügliches Eingreifen zu ermöglichen.

5 .2. Erfordernis einer Vorabgenehmigung der CNPD

Die Erfordernis einer Vorabgenehmigung spiegelt den ausdrücklichen Willen des luxemburgischen Gesetzgebers zum Schutz natürlicher Personen vor bestimmten Verarbeitungen wider, *„die besondere Gefahren für die Rechte und Freiheiten der betroffenen Personen darstellen könnten..."*[18]. Dazu zählen insbesondere Verarbeitungen im Bereich der Überwachung am Arbeitsplatz, da diese eine besondere Gefahr für die Privatsphäre der Arbeitnehmer am Arbeitsplatz darstellen.

Jeder für die Verarbeitung Verantwortliche, der den Einsatz einer Verarbeitung zu Überwachungszwecken plant, muss bei der CNPD eine Vorabgenehmigung beantragen. Die einzige Ausnahme von diesem Grundsatz ist der Fall einer Überwachung, die ausschließlich auf Dritte abzielt, d.h. eine Überwachung, die nicht an einem Arbeitsplatz durchgeführt wird und deren Daten nicht aufgezeichnet werden[19]. Diese Bedingung ist streng auszulegen, d.h. sobald ein Arbeitnehmer des für die Verarbeitung Verantwortlichen von der Überwachung betroffen ist, würde die Ausnahme nicht länger greifen und eine Vorabgenehmigung wäre dennoch erforderlich. Diese Ausnahme ist in der Praxis jedoch sehr selten. Für diese Art der Verarbeitung ist trotzdem die Einreichung einer Vorabmeldung bei der CNPD erforderlich.

18 Parlamentsdokument Nr. 4735/13, S. 29.

19 Art. 14, Abs. (1), Buchstabe (b) des Gesetzes.

Darüber hinaus ist noch die Sonderregelung aus Artikel 17 des Gesetzes anzumerken, die bestimmte Verarbeitungen nicht der Genehmigung der CNPD sondern der **Genehmigung auf dem Wege einer großherzoglichen Verordnung** unterstellt.

Dabei handelt es sich um die nachstehenden Datenverarbeitungen:

- Die Verarbeitungen allgemeiner Art seitens der großherzoglichen Polizei und der Zoll- und Akzisenverwaltung, die im Rahmen der Vorbereitung, der Ermittlung und der Feststellung von Straftaten durchgeführt werden;
- die seitens der großherzoglichen Polizei in den Sicherheitszonen öffentlicher Straßen betriebenen Videoüberwachungssysteme;
- die Verarbeitungen seitens der Armee;
- die Verarbeitungen seitens des Geheimdienstes.

Die Kontrolle und Überwachung all dieser Verarbeitungen fällt nicht in die Zuständigkeit der CNPD, sondern in die Zuständigkeit einer spezifischen Kontrollbehörde, die sich aus dem Generalstaatsanwalt und zwei Mitgliedern der CNPD zusammensetzt (für weitere Einzelheiten, siehe Artikel 17 des Gesetzes).

Schließlich sei angemerkt, dass das **Datenschutzgesetz nicht** für die von einer natürlichen Person im ausschließlichen Rahmen ihrer persönlichen oder häuslichen Aktivitäten vorgenommenen Datenverarbeitung **gilt**[20].

Das Gesetz findet demnach keine Anwendung, wenn eine Person beispielsweise an ihrem Wohnsitz Videokameras installiert, die jedoch in keinem Fall öffentliche Straßen oder angrenzenden Grundbesitz filmen dürfen.

In allen anderen Fällen obliegt der Nationalen Kommission im Rahmen ihrer Genehmigungsbefugnis insbesondere die Überprüfung der nachstehenden Bedingungen:

- Dass die Daten für festgelegte, eindeutige und zulässige **Zwecke** erhoben werden und nicht auf mit diesen Zweckbestimmungen unvereinbare Weise weiterverarbeitet werden,
- dass der für den Rückgriff auf die Überwachung geltend gemachte Grund einem gesetzlich vorgesehenen **Zulässigkeitskriterium** entspricht,
- dass die geplante Maßnahme im Hinblick auf die konkreten Umstände **notwendig** und nicht lediglich nützlich oder zweckmäßig ist (insbesondere dass die durch die Überwachung zu vermeidenden oder zu bekämpfenden Gefahren hinreichend real und erheblich sind). Diesbezüglich hat die luxemburgische Rechtsprechung präzisiert, dass eine bloße Zweckmäßigkeitserwägung nicht ausreichend ist[21]. Diese Rechtsprechung wurde in der Berufungsinstanz bestätigt[22].

20 Art. 3, Abs. (3) des Gesetzes.

21 ***Verwaltungsgericht Luxemburg, 15. Dezember 2004, Nr. 17890:*** *„Ein Gerät, dessen Einrichtung in vielerlei Hinsicht zweckmäßig erscheinen mag - beispielsweise aufgrund der Senkung der Diebstahlgefahr durch die abschreckende Wirkung von Kameras - ist noch lange nicht automatisch als notwendig zu betrachten. Die Notwendigkeit übersteigt die bloße Zweckmäßigkeit dahingehend, dass sie das betrifft, was man unbedingt benötigt und ohne das man nicht auskommen kann, das Unentbehrliche, also etwas, das über das hinausgeht, was lediglich zur Zeit, zum Ort und zu den Umständen passt und die bloße Zweckmäßigkeit kennzeichnet".*

22 ***Verwaltungsgerichtshof Luxemburg, 12. Juli 2005, Nr. 19234C, S. 11 f.,*** *„Die CNPD hat im vorliegenden Fall mit Recht die Notwendigkeit der Verarbeitung beurteilt, die Gegenstand des Antrags der Gesellschaft X in Bezug auf die seitens des Gesetzes in diesem Zusammenhang erschöpfend aufgezählten verschiedenen Vorbedingungen ist, da sie vom Gesetzgeber den klaren Auftrag erhalten hat, zu überprüfen, ob der der Vorabgenehmigung unterliegende Antrag unter die durch das Gesetz vorgesehenen Bestimmungen fällt. Es genügt folglich nicht, dass die Antragstellerin, im vorliegenden Fall die Berufungsklägerin, behauptet, mittels des von ihr geplanten Videoüberwachungssystems den Schutz ihrer Güter zu beabsichtigen. Sie muss hingegen den Nachweis der Richtigkeit ihrer Behauptungen erbringen. Folglich konnte die CNPD zu Recht die Analyse der seitens der Berufungsklägerin geltend gemachten Notwendigkeit durchführen und die in diesem Zusammenhang seitens der ersten Richter gezogenen Schlussfolgerungen sind zu bestätigen.".*

5

5. Wie sind die Arbeitnehmer geschützt?

- dass die Auswirkung der Überwachung auf die Grundrechte und Grundfreiheiten und insbesondere auf die Privatsphäre der betroffenen Personen im Verhältnis zum verfolgten Zweck erträglich und im Rahmen bleibt (**Verhältnismäßigkeit**) und es keine Alternativmaßnahmen gibt, die auf eine weniger in die Privatsphäre der der Überwachung ausgesetzten Personen eingreifende Weise zum erwünschten Ergebnis führen,
- dass die Daten **sicher** verarbeitet und nur so lange wie tatsächlich erforderlich **gespeichert** werden.

Die Entscheidungen der CNPD zielen darauf ab, ein angemessenes Gleichgewicht zwischen den verschiedenen betroffenen Interessen herzustellen. Mittels einer gründlichen und fallspezifischen Analyse wägt die CNPD die Interessen der betroffenen Personen ab, d.h. ihr Recht auf Schutz ihrer Privatsphäre sowie das berechtigte Interesse des Arbeitgebers an der Durchführung einer Verarbeitung zu Überwachungszwecken.

Die Rechtsprechung hat klar festgesetzt, dass die CNPD bei der von ihr zur Genehmigung der Datenverarbeitungen durchzuführenden Analyse über eine Ermessensbefugnis im Einzelfall verfügt. In einem Urteil des Verwaltungsgerichts aus dem Jahr 2004 wurde entschieden, dass die Aufgabe der CNPD genau darin besteht, von Fall zu Fall zu entscheiden. Das Argument, wonach sich die CNPD ausschließlich auf die formale Anwendung des Gesetzes beschränken müsste anstatt eine Beurteilung durchzuführen, wurde seitens des Gerichts wie folgt widerlegt: *„... der gegenüber der Kommission vorgebrachte Vorwurf, die Zweckmäßigkeit der Einrichtung des vorgeschlagenen Videoüberwachungssystems im vorliegenden Fall beurteilt und auf diese Weise ihre Befugnisse überschritten zu haben, ist unbegründet, da die CNPD dadurch im Gegenteil den seitens des Gesetzgebers vorgezeichneten Ansatz befolgt hat, indem sie die bestehende oder fehlende Notwendigkeit des geplanten Geräts im Verhältnis zum Bedürfnis der Arbeitnehmer nach Gesundheit und Sicherheit sowie im Verhältnis zum Bedürfnis nach dem Schutz der Unternehmensgüter beurteilt hat".*[23]

Diese seitens des Verwaltungsgerichts angenommene Position wurde in der Berufungsinstanz bestätigt[24]: *„Um die ihr seitens des Gesetzgebers so übertragene Aufgabe sicherstellen zu können, muss die CNPD notwendigerweise eine Kontrolle der Verhältnismäßigkeit der geplanten Maßnahmen durchführen, um entscheiden zu können, ob die so vorgeschlagene Verarbeitung zur Sicherstellung der gesetzlich vorgesehenen Bedürfnisse notwendig ist. Folglich war die CNPD weit davon entfernt, ihre gesetzlichen Befugnisse zu überschreiten und handelte nach Maßgabe des ihr seitens des Gesetzgebers übertragenen Auftrags, wie dies die ersten Richter zu Recht festgestellt haben."*

Die Genehmigungen der CNPD sind meistens an Bedingungen und/oder Empfehlungen geknüpft. Diese werden im Zusammenhang mit dem in nachstehendem Punkt 7. dargelegten verschiedenen Überwachungsarten genauer analysiert.

5.3. Seitens des Arbeitgebers einzuhaltende gesetzliche Verpflichtungen

Neben der Verpflichtung zur Einhaltung der Grundsätze der Zweckbindung, der Zulässigkeit, der Notwendigkeit und der Verhältnismäßigkeit, muss der für die Verarbeitung Verantwortliche vor der Umsetzung

23 ***Verwaltungsgericht Luxemburg, 15. Dezember 2004, Nr. 17890.***

24 ***Verwaltungsgerichtshof Luxemburg, 12. Juli 2005, Nr. 19234C.***

einer Verarbeitung zu Überwachungszwecken darüber hinaus auch auf einige inhaltliche und formale Erfordernisse achten.

Das abgeänderte Gesetz vom 2. August 2002 über den Datenschutz enthält bestimmte Erfordernisse, die jede Datenverarbeitung erfüllen muss. Der für die Verarbeitung Verantwortliche muss darauf achten, seiner *Informationspflicht* nachzukommen, d.h. die betroffenen Personen darüber in Kenntnis setzen, dass eine Verarbeitung ihrer Daten stattfindet. Darüber hinaus muss er ihnen das *Recht auf Auskunft, Löschung* und *Änderung* ihrer Daten gewährleisten und diese Daten unter gleichzeitiger Gewährleistung ihrer *Vertraulichkeit* und *Sicherheit* über eine *zeitlich begrenzte Dauer speichern*.

N.B.: Wir möchten unterstreichen, dass sämtliche der nachstehend untersuchten gesetzlichen Verpflichtungen selbstverständlich auf alle der später in Abschnitt 7 ausgeführten Überwachungsarten Anwendung finden, weshalb wir in den Punkten 7.1. bis 7.6. nicht mehr detailliert auf alle diese Verpflichtungen zurückkommen werden.

5.3.1. Verpflichtung zur Information der Arbeitnehmer und der Personalvertretung- Der Grundsatz der Transparenz

Information der Arbeitnehmer

Jeder für die Verarbeitung Verantwortliche ist dazu verpflichtet, die von der von ihm durchgeführten Verarbeitung betroffenen Personen klar und unmissverständlich darüber in Kenntnis zu setzen. Jeder Arbeitnehmer hat folglich das Recht[25] zu wissen, ob und zu welchen Zwecken seine personenbezogenen Daten verarbeitet werden. Die Arbeitnehmer müssen bei der Erfassung oder spätestens bei der Aufzeichnung der sie betreffenden Daten verpflichtend informiert werden.

Es gibt jedoch auch mehrere Ausnahmen vom Informationsrecht[26], insbesondere wenn die Verarbeitung zur Wahrung der Staatssicherheit, der Verteidigung und der öffentlichen Sicherheit, zur Vorbeugung, Ermittlung, Feststellung und Verfolgung von Straftaten, usw. erforderlich ist. In der Praxis können diese Ausnahmen seitens eines Arbeitgebers in Bezug auf eine Verarbeitung zu Überwachungszwecken nur selten geltend gemacht werden.

Der Grundsatz der Transparenz beinhaltet auch, dass **heimliche** Überwachungsmaßnahmen von einem für die Verarbeitung Verantwortlichen niemals eingesetzt und von der CNPD niemals genehmigt werden dürfen. Nach luxemburgischem Recht kann ausschließlich ein Untersuchungsrichter heimliche Überwachungsmaßnahmen anordnen (Art. 88-1 und 88-2 der Strafprozessordnung).

Information der Personalvertretung

Es genügt nicht, dass der Arbeitgeber lediglich die der Überwachung ausgesetzten Arbeitnehmer informiert. Das Gesetz sieht darüber hinaus vor, dass der gemischte Betriebsrat oder in Ermangelung dessen die Personalvertretung oder in Ermangelung auch dieser die Gewerbeinspektion gesondert über die Durchführung der Überwachung informiert wird. Dabei handelt es sich um eine verschärfte Informationspflicht, die im Rahmen einer Überwachung am Arbeitsplatz Anwendung findet[27].

Information Dritter

Wenn auch Dritte (bei denen es sich nicht um Arbeitnehmer handelt) von der Überwachung betroffen

25 Art. 26 des abgeänderten Gesetzes vom 2. August 2002.

26 Art. 27 des abgeänderten Gesetzes vom 2. August 2002.

27 Art. L.261-1, Abs. (2) des Arbeitsgesetzbuchs.

5

5. Wie sind die Arbeitnehmer geschützt?

sind, müssen diese gemäß Artikel 26 des Gesetzes selbstverständlich ebenfalls informiert werden.

5.3.2. Wahrung des Rechts auf Auskunft und Berichtigung

Der Arbeitnehmer kann von seinem Arbeitgeber die kostenlose und in angemessenen Zeitabständen und ohne übermäßige Verzögerung erfolgende Mitteilung der ihn betreffenden verarbeiteten Daten in verständlicher Form sowie sämtliche Informationen über die Herkunft dieser Daten verlangen. Darüber hinaus ist er auch zur Berichtigung oder Streichung falscher oder veralteter Daten berechtigt[28].

Wie beim Informationsrecht sieht das Gesetz auch in diesem Fall bestimmte Ausnahmen vom Auskunftsrecht der betroffenen Person vor[29]. In der Praxis können diese Ausnahmen seitens eines Arbeitgebers in Bezug auf eine Verarbeitung zu Überwachungszwecken nur selten geltend gemacht werden.

5.3.3. Begrenzte Speicherdauer

Der **Zeitraum**, in dem die verarbeiteten Daten in einer Form aufbewahrt werden, die die Identifizierung der betroffenen Personen ermöglicht, **darf den erforderlichen Zeitraum für die Durchführung der Zweckbestimmungen, für die die Daten erhoben und verarbeitet werden, nicht überschreiten**[30].

Die Speicherung oder Aufzeichnung der Daten muss folglich zeitlich begrenzt sein. Der Zweck der Datenverarbeitung dient dabei als Indikator für die Bestimmung der angemessenen Speicherzeit. Nach Ablauf der festgesetzten Speicherfrist sind die Daten grundsätzlich zu vernichten. Im Bereich der Videoüberwachung genehmigt die CNPD beispielsweise grundsätzlich eine achttägige Speicherfrist der Bilder. In Sonderfällen kann diese Frist gegebenenfalls auf bis zu maximal 30 Tage verlängert werden.

Natürlich müssen die Daten nach Ablauf der Speicherfrist nicht vernichtet werden, wenn sie an die zuständigen öffentlichen Behörden oder Justizbehörden zur Feststellung oder Verfolgung einer Straftat weitergeleitet werden[31] (beispielsweise Bilder, auf denen ein Ladendiebstahl zu sehen ist).

Anonyme oder anonymisierte Daten können über einen unbegrenzten Zeitraum gespeichert werden, wobei die Anonymisierung streng auszulegen ist und eine Pseudonymisierung oder Verschlüsselung nicht ausreicht. Die Anonymisierung muss **unumkehrbar** sein, d.h. so durchgeführt werden, dass die Person, auf die sich die Daten beziehen, ungeachtet der eingesetzten Mittel niemals wieder identifiziert werden kann.

5.3.4 Annahme angemessener Maßnahmen zur Gewährleistung der Sicherheit und Vertraulichkeit

Der für die Verarbeitung Verantwortliche muss hinreichende organisatorische und technische Sicherheitsmaßnahmen ergreifen, um den Schutz der verarbeiteten Daten gegen zufällige oder unrechtmäßige Vernichtung, zufälligen Verlust, Veränderung, unberechtigte Weitergabe oder unbefugten Zutritt, insbe-

28 Art. 28 des abgeänderten Gesetzes vom 2. August 2002.

29 Art. 29 des abgeänderten Gesetzes vom 2. August 2002.

30 Gemäß Artikel 4, Absatz (1), Buchstabe (d) des abgeänderten Gesetzes vom 2. August 2002.

31 Siehe Artikel 10, Absatz (3), Buchstaben (b) und (c) des abgeänderten Gesetzes vom 2. August 2002.

sondere wenn im Rahmen der Verarbeitung Daten in einem Netz übertragen werden, sowie gegen jede andere Form der unrechtmäßigen Verarbeitung zu gewährleisten[32].

Der für die Verarbeitung Verantwortliche muss überdies gewährleisten, dass die ihm untergeordneten Personen (Arbeitnehmer oder sonstige) die Daten unter Einhaltung der Bedingungen des abgeänderten Gesetzes vom 2. August 2002 verarbeiten.

Sofern er auf einen Auftragsverarbeiter zurückgreift, muss er sich darüber vergewissern, dass sein Leistungserbringer (Auftragsverarbeiter) ebenfalls die gesetzlich auferlegten Bedingungen für die Datensicherheit erfüllt. Der für die Verarbeitung Verantwortliche bleibt trotz des Rückgriffs auf einen solchen Auftragsverarbeiter jederzeit für die Verwendung dieser Daten verantwortlich.

Darüber hinaus ist noch anzumerken, dass die Sicherheitsmaßnahmen in Abhängigkeit von der Art der Überwachung, dem Stand der Technik und den mit ihrer Umsetzung verbundenen Kosten variieren können.

32 Gemäß Artikel 22 und 23 des abgeänderten Gesetzes vom 2. August 2002.

6

6. Wie wird die Nichteinhaltung der Rechtsvorschriften bestraft?

Die CNPD verfügt (im hier erörterten Bereich) über keine Befugnis zur Verhängung von Geldstrafen. Diese Befugnis besteht lediglich im Rahmen der Anwendung des Gesetzes vom 30. Mai 2005 betreffend die spezifischen Bestimmungen bezüglich des Schutzes der Person bei der Datenverarbeitung auf dem Gebiet der elektronischen Kommunikation und betreffend die Abänderung der Artikel 88-2 und 88-4 der Strafprozessordnung.

Sie verfügt jedoch über die Befugnis zur Verhängung bestimmter Verwaltungsstrafen gegen den für die Verarbeitung Verantwortlichen[33].

An dieser Stelle ist hervorzuheben, dass fast die Hälfte der Bestimmungen (19 von 45 Artikeln) des Datenschutzgesetzes bei Verstoß Strafmaßnahmen vorsehen. Der Einsatz oder die Verwendung eines Überwachungssystems, das gegen die Bestimmungen des Gesetzes oder die seitens der CNPD aufgestellten Bedingungen verstößt, kann demnach ein strafrechtliches Vergehen darstellen. Folglich kann es passieren, dass ein für die Verarbeitung Verantwortlicher von einem Gericht zu einer Freiheitsstrafe von acht Tagen bis zu einem Jahr sowie zu einem Bußgeld von Euro 251,- bis Euro 125 000,- oder lediglich zu einer dieser beiden Strafen verurteilt wird.

33 Artikel 33 des abgeänderten Gesetzes vom 2. August 2002.

7. Überwachungsarten

Nach der Analyse der Bedingungen und Erfordernisse, denen die Datenverarbeitung zu Überwachungszwecken unterliegt, befassen sich die nachstehenden Ausführungen mit der Erstellung eines Überblicks über die seitens der Arbeitgeber am häufigsten eingesetzten Überwachungsarten.

Die prozentuale Verwendung der seitens der CNPD genehmigten Überwachungsarten ist wie folgt (statistisches Mittel über einen Zeitraum von 10 Jahren):

- Videoüberwachung: 70 %
- Überwachung der Verwendung von IT-Tools: 7%
- Aufzeichnung von Telefongesprächen: 8,5%
- Biometrische Systeme: 1%
- Geolokalisierungsgeräte: 5%
- Überwachung des Zutritts zu Räumlichkeiten: 5%
- Kontrolle der Arbeitszeiten: 3,5%

7.1. Videoüberwachung

Immer mehr Arbeitsplätze sind mit Videoüberwachungsgeräten ausgestattet. Wenngleich diese Geräte zur Gewährleistung der Sicherheit der Arbeitnehmer oder zum Schutz der Unternehmensgüter als zulässig betrachtet werden können, stellen sie gleichzeitig auch einen Eingriff in die Privatsphäre der Personen dar und berühren die unbeobachtete Bewegungsfreiheit.

7.1.1. Welche Zielsetzungen kann der Arbeitgeber verfolgen?

Es gibt zahlreiche Gründe dafür, warum ein Arbeitgeber ein Videoüberwachungsgerät anbringen möchte:

- zum Schutz der Güter seines Unternehmens (z.B. Waren, Geld, Anlagen, Maschinen, Gebäude, vertrauliche Dokumente, usw...);
- zur Sicherheit des Personals, der Kunden;
- zur Identifizierung der Täter von Diebstählen und Überfällen;
- zur Absicherung des Zutritts zum Gelände oder zu den Gebäuden;
- zur Feststellung und Identifizierung von verdächtigen oder gefährlichen Verhaltensweisen, die zu Unfällen oder Vorfällen führen könnten;
- zur Ermittlung des Ursprungs von Vorfällen;
- zur Verständigung der Rettungsdienste, der Feuerwehr oder der Polizei;
- zur Ermöglichung einer schnellen Evakuierung im Ernstfall.

Diese Liste ist lediglich eine beispielhafte Aufzählung, da es zahlreiche weitere Gründe geben kann, die den Rückgriff auf ein Videoüberwachungssystem rechtfertigen.

Um akzeptiert zu werden, müssen diese Gründe oder Zweckbestimmungen mindestens einer der gesetzlich vorgesehenen Vorbedingungen entsprechen (siehe nachstehenden Punkt 7.1.2.). Darüber hinaus muss die CNPD die Notwendigkeit und die Verhältnismäßigkeit der seitens des Arbeitgebers geplanten Überwachungsmaßnahmen untersuchen, bevor sie ihm eine entsprechende Genehmigung erteilen kann (Punkt 7.1.3.).

7

7. Überwachungsarten

7.1.2. In welchen Fällen ist eine Videoüberwachung möglich?

7.1.2.1. Videoüberwachung der Arbeitnehmer

Der Arbeitgeber muss mindestens eine Zulässigkeitsbedingung aus Artikel L.261-1(1) des Arbeitsgesetzbuchs geltend machen[34] und nachweisen können. An dieser Stelle sei daran erinnert, dass die Überwachung der Arbeitnehmer am Arbeitsplatz nur dann möglich ist, wenn sie notwendig ist:

- für die Sicherheit und Gesundheit der Arbeitnehmer, oder
- zum Schutz der Unternehmensgüter, oder
- zur Kontrolle des Produktionsablaufs (ausschließlich auf Maschinenseite), oder
- für die zeitweilige Kontrolle der Produktion oder der Leistungen des Arbeitnehmers, sofern eine derartige Maßnahme das einzige Mittel zur Festlegung der genauen Bezahlung ist, oder
- im Rahmen der Arbeitsorganisation auf Basis von Gleitzeit nach Maßgabe des Arbeitsgesetzbuchs.

Sicherheit und Gesundheit der Arbeitnehmer

Im Rahmen dieser Vorbedingung muss der für die Verarbeitung Verantwortliche konkrete Situationen oder Faktoren in seinem Unternehmen nachweisen, die ihn zu der Erwägung veranlassen, dass die Sicherheit und/oder die Gesundheit seiner Arbeitnehmer (Beschäftigte, Praktikanten, Zeitarbeitskräfte, Lehrlinge) in Gefahr sein und das Videoüberwachungssystem zur Verhinderung dieser Gefahr beitragen könnte. Als Beispiele können das Vorhandensein gefährlicher Maschinen, giftiger oder schädlicher Stoffe angeführt werden, aber auch gefährliche Aufgaben wie im Falle von Mitarbeitern von Geld- und Werttransportunternehmen oder an der Kasse beschäftigten Bankangestellten, usw.

Das typische Beispiel sind dabei Arbeitnehmer, die an Tankstellen arbeiten. Wie die Kriminalitätsstatistiken bezeugen, stellt dieser öffentlich zugängliche Arbeitsplatz eine erhöhte Gefahr für bewaffnete Diebstähle dar. Darüber hinaus besteht aufgrund der Lagerung und Handhabung von großen Mengen leicht entzündlicher und gefährlicher Produkte (Kohlenwasserstoffe oder sonstige) ein Explosions- oder Brandrisiko. Ein Videoüberwachungssystem kann zur Verhinderung der damit verbundenen Unfälle, aber auch zur Abschreckung vor Raubüberfällen und folglich vor Angriffen auf die körperliche Unversehrtheit der Arbeitnehmer beitragen.

Schutz der Unternehmensgüter

Dieses Zulässigkeitskriterium betrifft vor allem Überwachungen, die auf die Verhinderung der Schädigung materieller Güter abzielen, d.h. auf die Verhinderung von Diebstählen und Vandalismus. In Bezug auf die Auslegung des Begriffs *„Schutz der Unternehmensgüter"* seitens der CNPD wird auf Punkt 5.1.1. verwiesen.

Dies betrifft insbesondere seitens der Arbeitnehmer begangene Diebstähle aus Kassen, Lagern, usw.

Kontrolle des Produktionsablaufs (ausschließlich auf Maschinenseite)

Diese dritte Vorbedingung bezieht sich auf die lediglich beiläufig erfolgende Überwachung der Arbeitnehmer im Zuge der hauptsächlichen Überwachung eines mechanischen und/oder automatisierten Fertigungssystems, wie beispielsweise eines automatisierten Bands zum Zusammenbau von Autoteilen oder eines automatischen Flaschenbefüllungssys-

34 Für weitere Informationen siehe Punkt 5.1.1.

tems eines Getränkeherstellers. Eine derartige Videoüberwachung kann nur dann auf Grundlage dieser Zulässigkeitsbedingung genehmigt werden, wenn sie die Feststellung eines eventuellen Produktionsfehlers und/oder einer Unterbrechung der Fertigungslinien ermöglicht und auf diese Weise die Kontrolle des Produktionsablaufs erlaubt. Die Videoüberwachung ist demnach in erster Linie zur Überwachung der Maschinen einzustellen und die Arbeitnehmer könnten lediglich rein beiläufig und zufällig das Sichtfeld der Kameras kreuzen, wie beispielsweise bei der Kontrolle des Maschinenbetriebs oder bei der Durchführung von Reparaturarbeiten.

Die beiden übrigen im Gesetz vorgesehenen Vorbedingungen finden in der Praxis selten oder nie Anwendung. Nach Ansicht der CNPD, ist der Fall der **zeitweiligen Kontrolle der Produktion oder der Leistungen des Arbeitnehmers, sofern eine derartige Maßnahme das einzige Mittel zur Festlegung der genauen Bezahlung ist**, in der Praxis nicht umsetzbar. In der Tat betrifft das einzig denkbare Beispiel Arbeitnehmer, die an einer Fertigungslinie tätig sind und in Abhängigkeit von der Anzahl der hergestellten Teile bezahlt werden. Diesbezüglich ist jedoch zunächst anzumerken, dass es wenig wahrscheinlich ist, dass diese Tätigkeits- und Bezahlungsart im Großherzogtum Luxemburg heutzutage noch existiert. Danach muss man sich bewusst machen, dass die Bestimmung der genauen monatlichen Bezahlung unmöglich ist, wenn die Videoüberwachung nur zeitweise eingesetzt werden kann.

An dieser Stelle ist anzumerken, dass die Arbeitgeber diese Zulässigkeitsbedingung jedoch häufig geltend machen. Dies scheint daran zu liegen, dass die Arbeitgeber der Ansicht sind (oder sein möchten), dass die Videoüberwachung zur Kontrolle der Produktion oder der Leistungen des Arbeitnehmers durchgeführt werden kann, ohne sich jedoch darüber im Klaren zu sein, dass sie lediglich erlaubt ist, wenn es sich dabei um eine **zeitweilige** Maßnahme handelt, die das **einzige Mittel** zur Festlegung der **genauen Bezahlung** darstellt.

Was die **Verarbeitung im Rahmen der Arbeitsorganisation auf Basis von Gleitzeit nach Maßgabe des Arbeitsgesetzbuchs** betrifft, so gibt es nach Ansicht der CNPD andere und weniger stark in die Privatsphäre eingreifende Mittel, die der Arbeitgeber anstelle der Videoüberwachung zur Kontrolle der Arbeits- und Anwesenheitszeiten seiner Arbeitnehmer einsetzen kann. Demnach sind die zur Überprüfung der Anwesenheitszeiten am Arbeitsplatz eingesetzten Videoüberwachungssysteme grundsätzlich nicht erlaubt, da eine Kontrolle der Arbeitszeit über Zutrittsausweise wirksamer ist und die Privatsphäre der Arbeitnehmer besser schützt.

7.1.2.2. Videoüberwachung von Personen, bei denen es sich nicht um Arbeitnehmer handelt

Wenn Personen, bei denen es sich nicht um Arbeitnehmer handelt (beispielsweise Kunden, Besucher, Lieferanten, Berater, usw.), von den Kameras gefilmt werden, muss der Arbeitgeber ebenfalls mindestens eine Zulässigkeitsbedingung aus Artikel 10 (1) des abgeänderten Gesetzes vom 2. August 2002 geltend machen und nachweisen. Dies trifft häufig auf Unternehmen zu, die mit freiem Zutritt für die breite Öffentlichkeit geöffnet sind, wie beispielsweise gewerbliche Einrichtungen oder Behörden.

Für die verschiedenen Zulässigkeitskriterien und Beispiele wird auf Abschnitt 5.1.2. verwiesen.

7.1.3. Die an Bedingungen geknüpfte Vorabgenehmigung der CNPD

Der für die Verarbeitung Verantwortliche muss für die Anbringung eines Videoüberwachungssystems bei der CNPD eine Vorabgenehmigung beantragen.

7

7. Überwachungsarten

Sofern die Zweckbestimmungen einer Datenverarbeitung über Videokameras eine oder mehrere Zulässigkeitsbedingungen erfüllen, führt die CNPD danach von Fall zu Fall und für jeden überwachten *„Bereich"* eine genaue Analyse der Notwendigkeit und der Verhältnismäßigkeit durch.

Die Analyse der Notwendigkeit einer Videoüberwachung erfordert insbesondere eine Untersuchung der Alternativen, die dem für die Verarbeitung Verantwortlichen die Erzielung derselben Zwecke unter Einsatz von weniger stark in die Privatsphäre der betroffenen Personen eingreifenden Mitteln ermöglichen. Nach Ansicht der Arbeitsgruppe *„Artikel 29"*[35], können diese Alternativen in *„Vorsorge-, Schutz-, und/oder Sicherheitsmaßnahmen physischer und/oder programmgesteuerter Art bestehen, die keine Bildaufnahmen erfordern, wie beispielsweise... Zutrittsfreigabegeräte, gewöhnliche Alarmsysteme..."*[36].

An dieser Stelle sei daran erinnert, dass der Grundsatz der Verhältnismäßigkeit beinhaltet, dass der für die Verarbeitung Verantwortliche die Verarbeitung auf Daten beschränken muss, die in Anbetracht der zu erzielenden Zweckbestimmungen angemessen und zutreffend sind und nicht darüber hinausgehen[37], und die Verarbeitungen nicht unverhältnismäßig sein dürfen.

In einigen Installationsbereichen können die Rechte der betroffenen Personen Vorrang vor der Notwendigkeit zur Einrichtung einer Videoüberwachung haben. Der Einbau einer Überwachungskamera in einem Büro, in dem ein Arbeitnehmer ständig arbeitet, ist beispielsweise als unverhältnismäßig oder übertrieben zu betrachten, da die Grundrechte und Grundfreiheiten der Arbeitnehmer Vorrang vor den seitens des Arbeitgebers verfolgten Interessen haben. Der Einbau von Videokameras in einer Restaurantküche wird ebenfalls als unverhältnismäßig und/oder übertrieben betrachtet, wenn man bedenkt, dass sich sämtliche in der Küche beschäftigten Arbeitnehmer nahezu permanent im Sichtfeld dieser Kameras befinden.

Mehrere Rechtsprechungen ahnden die fehlende Genehmigung der CNPD mit strafrechtlichen Sanktionen: **Bezirksgericht Luxemburg, 24. April 2008, Nr. 1342/2008; Bezirksgericht Luxemburg, 27. Oktober 2008, Nr. 3055/2008; Bezirksgericht Luxemburg, 21. Oktober 2010, Nr. 3429/2010.**

In anderen Entscheidungen wird zunächst die Frage nach der Zulässigkeit und Statthaftigkeit des Beweismittels der Bilderaufzeichnungen in Ermangelung der seitens der CNPD gewährten Vorabgenehmigung aufgeworfen. Ohne Vorabgenehmigung kann die Verarbeitung dieser Bilder (und folglich auch der Einsatz dieser Bilder als Beweismittel vor Gericht) unter Umständen ein strafbares Vergehen darstellen (Freiheitsstrafe und/oder Bußgeld). Das Urteil, das diese Problematik aufwirft und zu dem Ergebnis gelangt, derartige „rechtswidrige" Beweismittel abzulehnen, ist das Urteil in der Rechtssache „Hauptpost", **Bezirksgericht Luxemburg, 13. Juli 2006, Nr. 2523/2006**, das in der Berufungsinstanz bestätigt wurde, **Berufungsgericht Luxemburg, 28. Februar 2007, Nr. 126/07X**. Diese beiden Urteile wurden jedoch durch ein Urteil des Kassationshofs aufgehoben, **Kassationshof Luxemburg, 22. November 2007, Nr. 57/2007.**

Weit entfernt von der Schaffung der Rechtssicherheit, die man sich in diesem Bereich erwarten würde, folgen bestimmte Entscheidungen im Hinblick auf die Zulässigkeit und Statthaftigkeit solcher Bilder bei fehlender Genehmigung nun der Argumentation des Kassationshofs (siehe insbesondere: **Bezirksgericht Luxemburg, 26. Juni 2008, Nr. 2202/2008; Bezirksgericht Luxemburg, 12. August 2008, Nr. 2614/2008; Berufungsgericht Luxemburg, 9. November 2010, Nr. 446/10V; Bezirksgericht Luxemburg, 1. Februar 2012, Nr. 534/2012)**, während andere eine komplett

35 *Arbeitsgruppe, die aus den Datenschutzbehörden der Europäischen Union besteht.*

36 *Siehe die am 11. Februar 2004 angenommene Stellungnahme 4/2004 der „Artikel 29"-Arbeitsgruppe zur Verarbeitung personenbezogener Daten mittels Videoüberwachung (WP 89, Seiten 16 bis 18).*

37 *Artikel 4, Absatz (1), Buchstabe (b) des Gesetzes.*

andere Argumentation verwenden, um trotzdem zum selben Ergebnis zu gelangen (**Bezirksgericht Luxemburg, 2. Februar 2009, Nr. 387/2009, bestätigt durch Berufungsgericht Luxemburg, 9. Juni 2009, Nr. 288/09V; Berufungsgericht, 16. Juni 2009, Nr. 313/09V**).

Eine interessante Rechtsprechung bleibt noch zu erwähnen, die zu dem Ergebnis gelangt, dass das Recht auf ein faires Verfahren verletzt worden wäre, sofern die ohne Genehmigung der CNPD aufgezeichneten Bilder als Beweismittel zugelassen worden wären. Diese Schlussfolgerung stützt sich insbesondere auf eine genaue Analyse der Einhaltung der seitens des abgeänderten Gesetzes vom 2. August 2002 gestellten Bedingungen und insbesondere der seitens des für die Verarbeitung Verantwortlichen geltend gemachten Zweckbestimmungen sowie der Einhaltung des Vorabinformationsrechts der Arbeitnehmer, das dadurch gestärkt wird (**Bezirksgericht Luxemburg, 16. Oktober 2008, Nr. 2925/2008**).

Im Rahmen der von ihr im Bereich der Videoüberwachung erteilten Genehmigungen kann die CNPD wohlgemerkt dazu veranlasst sein, bestimmte Bereiche abzulehnen, sofern die Bedingungen des Gesetzes oder die Grundsätze der Notwendigkeit und der Verhältnismäßigkeit nicht eingehalten werden. Unter Einsatz ihrer Ermessensbefugnis setzt sie in diesen Genehmigungen darüber hinaus Bedingungen und Erfordernisse fest, die wie folgt zusammengefasst werden können:

7.1.3.1. Verbot einer ständigen und ununterbrochenen Überwachung (außer in seltenen Ausnahmefällen)

Grundsätzlich **erlaubt das Gesetz nicht, die Arbeitnehmer einer ständigen und ununterbrochenen Überwachung an ihrem Arbeitsplatz auszusetzen**. Die parlamentarischen Arbeiten präzisieren diesbezüglich, dass *„die Überwachung an das verfolgte zulässige Ziel angepasst sein muss. Der Arbeitgeber muss auf Überwachungsmittel zurückgreifen, die die Privatsphäre des Arbeitnehmers am besten schützen. Die Einhaltung dieses Grundsatzes der Verhältnismäßigkeit erfordert, dass beispielsweise automatische und ununterbrochene Überwachungen der Arbeitnehmer zu vermeiden sind*[38] *"*.

So ist der Betreiber eines Restaurants beispielsweise nicht dazu berechtigt, seine Arbeitnehmer unter Geltendmachung des Schutzes seiner Unternehmensgüter in der Küche zu überwachen. Die Arbeitnehmer unterstünden nahezu permanent der Videoüberwachung und es ist ganz offensichtlich, dass eine derartige Überwachung für die sich beobachtet fühlenden und wissenden Arbeitnehmer einen erheblichen psychischen Druck erzeugen kann, der immer stärker wird, je länger die Maßnahmen anhalten. Die Tatsache, dass die Arbeitnehmer über kein Mittel verfügen, sich dieser Überwachung hin und wieder zu entziehen, verschlimmert diesen Druck zusätzlich. Eine derartige ständige Überwachung wird im Verhältnis zum beabsichtigten Zweck als unverhältnismäßig betrachtet und stellt eine übermäßige Verletzung der Privatsphäre des Arbeitnehmers am Arbeitsplatz dar. In diesem Fall müssen die Grundrechte und Grundfreiheiten der Arbeitnehmer Vorrang vor den seitens des Arbeitgebers verfolgten Interessen haben.

Zur Vermeidung einer ständigen Überwachung reicht es häufig aus, das Sichtfeld der Kameras auf die Fläche zu begrenzen, die für die Verfolgung der Zweckbestimmung des Schutzes der Unternehmensgüter oder der Sicherheit des Personals erforderlich ist. Auf diese Weise ist beispielsweise die Kameraüberwachung eines Kassenbereichs nach wie vor möglich, sofern die Kameras so eingestellt sind, dass sie nicht auf die Arbeitnehmer ausgerichtet sind. Die besagten Kameras müssen für das Personal so unaufdringlich wie möglich ausgerichtet sein, d.h. unter Begren-

38 Siehe Parlamentsdokument Nr. 4735/13, S. 22 und 23

7

7. Überwachungsarten

zung ihres Sichtfelds auf allein die Bereiche, in denen Bargeld oder Bankkarten zum Einsatz kommen, d.h. auf die Kassen selbst, auf die Kassenschubladen und gegebenenfalls auf die Unterarme der Arbeitnehmer. Wenn es stimmt, dass die Bilder der Videoüberwachung die Identifizierung der Täter eventueller Angriffe ermöglichen müssen, ist die Kameraüberwachung der am Schalter anwesenden Arbeitnehmer noch lange nicht erforderlich. Daher reicht es nach Ansicht der CNPD aus, dass die Kameras auf die Vorderseite des Ladentischs ausgerichtet sind, d.h. den Wartebereich der sich vor dem Ladentisch befindenden Kunden einfangen. Die Sichtfelder der verschiedenen Kameras dürfen folglich die Arbeitsplätze der hinter dem Ladentisch beschäftigten Arbeitnehmer nicht beinhalten.

In bestimmten Fällen kann die Gefahr für die Sicherheit des Personals hingegen so bedeutend sein, dass sie Vorrang vor dem Schutz ihrer Privatsphäre hat. Da Raubüberfälle in Banken häufig mit Gewalt einhergehen, kann es folglich gerechtfertigt sein, dass bestimmte und insbesondere die an den Kassenschaltern tätigen Arbeitnehmer, ständig überwacht werden. Die CNPD ist jedoch der Ansicht, dass das Sichtfeld der Kameras soweit möglich auf keinen bestimmten Arbeitnehmer ausgerichtet sein darf. Sofern dies aufgrund der örtlichen Gegebenheiten absolut nicht zu vermeiden ist, darf der betreffende Arbeitnehmer nicht von vorn gefilmt werden.

Eine ständige Überwachung von Personen, bei denen es sich nicht um Arbeitnehmer handelt, wirft dieselbe Problematik auf und ist nicht immer zulässig. So erteilt die CNPD keine Genehmigung für das Filmen im Inneren eines Restaurants unter Einbeziehung der Esstische. Selbst wenn im Speisesaal eines Restaurants ein bestimmtes Diebstahl- oder Vandalismusrisiko bestehen kann, macht dieses eine Videoüberwachung noch lange nicht automatisch erforderlich. Die anwesenden Gäste wären ständig videoüberwacht, wenn sie ein Restaurant als Treffpunkt für gesellige Momente wählen, um sich zu unterhalten, Spaß zu haben oder sich zu entspannen. Die Gäste, die über einen mehr oder weniger langen Zeitraum an diesem Ort verweilen, müssen berechtigterweise erwarten können, während dieser privaten Momente nicht gefilmt zu werden. Durch den Einsatz von Kameras im Speisesaal eines Restaurants unter Einbezug der Esstische könnte das Verhalten aller an einem Tisch sitzenden Gäste gefilmt werden, was bei den Gästen Unbehagen oder gar psychischen Druck hervorrufen könnte, da sie sich während ihres gesamten Aufenthalts im Restaurant beobachtet fühlen. Eine solche ständige Überwachung ist in Bezug auf den beabsichtigten Zweck als unverhältnismäßig zu betrachten und stellt eine Gefährdung der Privatsphäre des Gastes dar.

Die deutsche Rechtsprechung hat im selben Sinn entschieden. So entschied ein Urteil des Amtsgerichts Hamburg vom 22. April 2008 in einem Videoüberwachungsfall beispielsweise, einer Café-Brasserie-Handelskette die Überwachung des Kundenbereichs ihrer Einrichtungen zu verbieten. Das Gericht begründete seine Entscheidung wie folgt: *„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. Verbot der Aufzeichnung des zu den Bildern gehörenden Tons

Eine über Videokameras erfolgende Überwachung darf lediglich die Bilder unter Ausschluss des Tons betreffen. Die Aufzeichnung des zu den Bildern gehörenden Tons stellt einen noch größeren Eingriff in die Privatsphäre dar, weshalb diese Art der Aufzeichnung generell verboten ist.

7.1.3.3. Verbot der Überwachung der Leistungen und des Verhaltens der Arbeitnehmer

Bei allen von ihr erteilten Genehmigungen hebt die Nationale Kommission insbesondere hervor, dass die Überwachung nicht zu der über die Zwecke, auf die die Genehmigung gründet, hinausgehenden Beobachtung des Verhaltens und der Leistungen der Arbeitnehmer des für die Verarbeitung Verantwortlichen dienen darf.

Folglich ist ein Arbeitgeber dazu berechtigt, die aus einem zum Zweck des Schutzes der Unternehmensgüter genehmigten Videoüberwachungssystem stammenden Bilder eines Arbeitnehmers, der einen Warendiebstahl begeht, zu verwenden. Er ist jedoch nicht dazu berechtigt, Maßnahmen gegen einen Arbeitnehmer einzuleiten, wenn dieser nach Ansicht des Arbeitgebers zu lange mit einem Kunden oder einem Arbeitskollegen spricht und dieses Verhalten vom Videoüberwachungssystem aufgezeichnet wird. Dies würde eine vom Gesetz verbotene Zweckentfremdung darstellen und dürfte grundsätzlich als Beweismittel vor Gericht nicht zugelassen werden.

7.1.3.4. Verbot des Filmens der den Arbeitnehmern zur privaten Nutzung vorbehaltenen Örtlichkeiten

Die CNPD verweigert es auch, dass die Überwachungskameras die den Arbeitnehmern zur privaten Nutzung vorbehaltenen oder nicht zur Erfüllung von Arbeitsaufgaben vorgesehenen Örtlichkeiten filmen, wie beispielsweise die Toiletten, die Garderoben, die Raucherecken, die Ruhezonen, den der Personalvertretung zur Verfügung gestellten Raum, die Küche/Kochecke, usw..

7.1.3.5. Begrenztes Sichtfeld der Kameras, die die internen und externen Zugänge oder die Umgebung eines Gebäudes oder Standorts filmen

Das Sichtfeld der zum Filmen eines Zutrittsortes (Ein- und Ausgang, Türschwelle, Eingangstreppe, Tür, Vordach, Eingangshalle, usw.) vorgesehenen Kameras muss auf die für die Anzeige der gerade eintretenden Personen (interne Zugänge) unbedingt erforderliche Fläche begrenzt ist. Die zum Filmen der externen Zugänge vorgesehenen Kameras dürfen nicht die gesamte Breite eines gegebenenfalls am Gebäude des Unternehmers oder an den angrenzenden öffentlichen Straßen entlanglaufenden Bürgersteigs einfangen.

Die an den Zufahrten oder in der Umgebung eines Gebäudes angebrachten Außenkameras müssen so eingestellt sein, dass sie die öffentliche Straße und die Zufahrten, Eingänge, Zugänge und Innenräume anderer möglicherweise in ihrem Sichtfeld liegenden Gebäude nicht einfangen.

7

7. Überwachungsarten

7.1.3.6. Begrenzte Speicherdauer der Bilder

Das Datenschutzgesetz sieht vor, dass die Daten nicht länger gespeichert werden dürfen als über den Zeitraum, der für die Erfüllung der Zwecke erforderlich ist, für die die Daten erfasst wurden. Was die Videoüberwachung betrifft, so ist die CNPD der Ansicht, dass die Bilder grundsätzlich über einen Zeitraum von bis zu 8 Tagen gespeichert werden können. In bestimmten Fällen können sie je nach Einzelfall länger gespeichert werden, wobei die Speicherzeit jedoch eine Frist von 30 Tagen nicht übersteigen darf.

Nach Ablauf der besagten Frist müssen die Daten unbedingt vernichtet werden. In Bezug auf die Speicherdauer einer als Beweiselement im Rahmen einer Straftat verwendeten Bildsequenz wird auf Punkt 5.3.1.3. verwiesen.

7.1.3.7. Überblick über die Videoüberwachungsbereiche

Obgleich die nachstehende Liste einen allgemeinen Überblick darüber gibt, in welchen Bereichen eine Videoüberwachung erlaubt ist oder nicht, sei dennoch daran erinnert, dass die CNPD in Abhängigkeit von den Besonderheiten des konkreten Falles eine andere Entscheidung treffen kann.

Grundsätzlich genehmigte Bereiche:

- von Ausnahmen abgesehen, alle Arten von Zugängen (diese Bereiche müssen auf die unbedingt erforderliche Fläche begrenzt sein);
- die Räume für die Warenlagerung / die Vorratsräume / die Lagerhäuser / die Lagerhallen oder Lagerschuppen (außer es gibt Arbeitnehmer, die ständig zur Arbeit im Lager eingeteilt sind, wie beispielsweise Lageristen);
- die Verkaufsräume oder Verkaufsflächen / die Regale / die Einkaufspassage / der Ausstellungsraum / der Verkaufs- und Beratungsraum (mit Ausnahme der Arbeitsplätze hinter einem Ladentisch);
- der Parkplatz (intern / extern / Tiefgarage);
- die Liefer- oder Ladezonen / die Liefer- und Entladerampen;
- der Computerraum / der Serverraum;
- die Gänge (außer in Hotels – Sondersituation);
- die Autowaschanlage / der Carwash;
- die Zapfsäulen;
- der Safe / der Sicherheitsraum / die Schließfächer;
- die Räumlichkeiten der Geldtransportunternehmen / der Raum der Geldtransportfahrer / der Raum des Geldtransporters;
- die Produktionsmaschinen (ausschließlich die Maschinen);
- die rein technischen Anlagen;
- der Betriebsraum / der Wartungsraum / der Zählerraum;
- die Archive;
- die Geldautomaten / die Bankautomaten.

Grundsätzlich nicht genehmigte Bereiche:

- öffentliche Straßen / Gehwege (Ausnahmegenehmigung im Falle einer besonderen Beschaffenheit der Örtlichkeiten; das Sichtfeld darf jedoch lediglich einen sehr begrenzten Teil der öffentlichen Straße umfassen);
- das angrenzende Gelände oder Gebäude;
- das Innere eines Büros / eines Arbeitsplatzes;
- der übliche Versammlungsraum;
- der Ruhe- oder Aufenthaltsraum;
- der Sportraum;

- die Toiletten / die Sanitäranlagen / die Duschen;
- das Büro der Personalvertretung;
- die Kochecke / das Raucherzimmer;
- die Garderobe / der Umkleideraum;
- die Stechuhr des Personals;
- der Speisesaal eines Gastronomiebetriebs oder der Verzehrraum eines Schankbetriebs;
- die Küche / das Innere der Küche;
- die Kantine / der Speiseraum / die Bar / die Imbissstube / das Café / die Terrasse / die Cafeteria;
- die Verzehrtheke eines Restaurants (ohne Kasse);
- die Werkstatt einer Autowerkstatt / die Produktionswerkstatt / die Arbeitswerkstatt / die Einbau- / Ausbauwerkstatt.

Bereiche, für die die Genehmigung der CNPD in Abhängigkeit von den jeweiligen Umständen, der Art, der Lage und der Beschaffenheit der Örtlichkeiten variiert; diese Bereiche sind im Allgemeinen Gegenstand von seitens der CNPD festgesetzten Bedingungen und Einschränkungen; in Abhängigkeit vom jeweiligen Einzelfall kann die Genehmigung zur Überwachung dieser Bereiche auch verweigert werden:

- die unmittelbare Umgebung, der Vorplatz;
- das Wartezimmer;
- der Kassenraum / der Raum der Kassenstandszählung / der Geldverarbeitungsraum;
- die Eingangshalle / die Rezeption / der Empfangsraum;
- die gemeinsam genutzten Teile eines Gebäudes;
- der Abfallraum / der Müllraum;
- der Pausenhof (und Umgebung);
- der Konzertsaal;
- das Zwischengeschoss, das Atrium;
- das Schwimmbad;
- das Gebäudedach;
- die Schalter.

7.2. Überwachung der Verwendung von IT-Tools

Der seit Ende der 1990er Jahre in den Unternehmen verzeichnete Aufschwung der neuen Informations- und Kommunikationstechnologien hatte zur Folge, dass die Arbeitnehmer in zunehmendem Maße IT-Tools (Internet, E-Mails, usw.) zu beruflichen wie auch zu privaten Zwecken nutzen.

Aus Sicht des Arbeitgebers wird die Überwachung dieser Instrumente häufig als Notwendigkeit für die Sicherheit seiner IT-Systeme betrachtet. Durch diese *„Cyber-Überwachung"* kann potenziellen Eingriffen in das IT-System oder Viren entgegengetreten werden. Die Arbeitnehmer betrachten diese Kontrolle häufig als übertrieben und als Eingriff in ihre Privatsphäre.

Es liegt auf der Hand, dass der Arbeitnehmer seinen Arbeitsvertrag ausführen und seine Loyalitätsverpflichtung gegenüber seinem Arbeitgeber erfüllen muss. Dennoch hat er auch das Recht auf den Schutz seiner Privatsphäre am Arbeitsplatz. Dieses Recht umfasst insbesondere das Briefgeheimnis.

Diese Rechte wurden in der Rechtsprechung insbesondere durch nachstehende Urteile präzisiert: **EGMR, Halford gegen Vereinigtes Königreich, 27.07.1997 und Kassationshof (Frankreich), Kammer für soziale Angelegenheiten, 2. Oktober 2001, Nikon**.

7

7. Überwachungsarten

7.2.1. Welche Zielsetzungen kann der Arbeitgeber verfolgen?

Der massive Einsatz von neuen Technologien am Arbeitsplatz kann bei den Arbeitgebern Besorgnis hervorrufen, da die Möglichkeit der Verbindung der Netze untereinander das IT-System anfälliger für Angriffe von außen oder für die Verbreitung von sensiblen oder vertraulichen Informationen macht.

Dieses Risiko könnte die vertraulichen Daten des Unternehmens und seiner Arbeitnehmer gefährden und wird durch die nachstehenden Faktoren noch verstärkt:

- die derzeitigen Nutzungsformen des Internet (Blogs, Foren, soziale Netzwerke, Instant Messaging...);
- die Nutzung tragbarer Geräte (USB-Stick, externe Festplatte, Laptop, Smartphone...) und
- das BYOD-Konzept (*„Bring Your Own Device"* – Bringen Sie Ihr privates Gerät mit), in dessen Rahmen der Arbeitnehmer seine privaten Geräte (Telefon, Laptop, Tablet-PC) im beruflichen Umfeld verwenden kann.

Der Arbeitgeber hat demnach berechtigtes Interesse daran, seine IT-Infrastrukturen durch die Überwachung der Verwendung der IT-Tools am Arbeitsplatz zu schützen. Seine Zielsetzungen können dabei insbesondere darin bestehen,

- zu vermeiden, dass vertrauliche Daten an Dritte verbreitet oder weitergeleitet werden, oder schlichtweg,
- über ein ordnungsgemäß funktionierendes IT-System zu verfügen (Blockade von Malware, Verhinderung von Datenstaus und Systemüberlastungen,...).

Sofern der Arbeitgeber im Allgemeinen die Verwendung der verschiedenen IT-Tools zu nicht-beruflichen Zwecken gestattet, muss diese Verwendung in einem vernünftigen Rahmen bleiben und darf den ordnungsgemäßen Betrieb des Unternehmens nicht beeinträchtigen.

7.2.2. In welchen Fällen ist die Überwachung der IT-Tools möglich?

Der Arbeitgeber kann die Verwendung der IT-Tools seitens der Arbeitnehmer nur dann überwachen, wenn diese Überwachung *„zum Zweck des Schutzes der Unternehmensgüter"* erfolgt. Dies ist grundsätzlich die einzige Bedingung, unter der eine solche Überwachung gerechtfertigt werden kann.

In Bezug auf Mitarbeiter, bei denen es sich nicht um Angestellte des Arbeitgebers handelt, ist die Überwachung nur möglich, wenn die betroffene Person ihre Einwilligung erteilt hat.

Bei der oben genannten Einwilligung muss es sich um eine freie, spezifische und in Kenntnis der Sachlage abgegebene Willensbekundung handeln[39]. Im vorliegenden Fall ist die Einwilligung der externen Mitarbeiter von jedem einzelnen externen Mitarbeiter über eine Klausel, Charta oder Police einzuholen, die die elektronische Überwachung während ihrer Tätigkeiten oder Dienstleistungen vorsieht. Die bloße Erwähnung (des Vorhandenseins) einer solchen Klausel, Charta oder Police seitens des für die Verarbeitung Verantwortlichen reicht nicht aus.

39 Artikel 2 (c) des abgeänderten Gesetzes vom 2. August 2002.

7.2.3. Die an Bedingungen und Empfehlungen geknüpfte Vorabgenehmigung der CNPD

Der CNPD obliegt die genaue Analyse der Genehmigungsanträge im Hinblick auf die Überwachung der Verwendung der IT-Tools zur Abwägung zwischen den Interessen des Unternehmens und dem Recht der Arbeitnehmer auf den Schutz ihrer Privatsphäre.

Dabei untersucht sie zunächst, ob die seitens des Arbeitgebers verfolgten Ziele dem Kriterium des Schutzes der Unternehmensgüter entsprechen.

Diesbezüglich präzisieren die Parlamentsdokumente, dass *„...zum Schutz der Unternehmensgüter auch die Überwachungsmittel zählen, die dazu dienen, sicherzustellen, dass keine Viren in das Computernetzwerk eindringen, dass keine Geschäftsdateien vernichtet werden, und dass das Netz nicht überlastet ist"*[40].

Nach Ansicht der CNPD umfasst der Begriff *„Schutz der Unternehmensgüter"* die materiellen Güter (d.h. die beweglichen und unbeweglichen Güter) des Unternehmens, nicht aber den Schutz anderer als der in Verbindung mit klar identifizierbaren materiellen oder immateriellen Gütern stehenden wirtschaftlichen Interessen des Unternehmens. Die Geltendmachung der Gefahr finanzieller Schäden, ungerechtfertigter Kosten oder entgangener Gewinne ist als Rechtfertigung unzureichend.

Aus den parlamentarischen Arbeiten geht hervor, dass die Sicherheit und/oder der ordnungsgemäße technische Betrieb der IT-Systeme des Unternehmens sowie der physische Schutz der Einrichtungen des Unternehmens (z.B. Systemüberlastungen, Verbreitung von Viren, Spoofing, usw.) eingeschlossen werden können.

Darunter fallen auch die immateriellen Güter wie die Rechte des geistigen Eigentums, die Betriebs- und Herstellungsgeheimnisse sowie die vertraulichen Informationen.

Andere Zweckbestimmungen wie die Kontrolle der Einhaltung des Ethik-Kodexes des Unternehmens (insbesondere die Verhinderung rechts- und sittenwidriger Verhaltensweisen, der Besuch pornographischer, pädophiler und rassistischer Webseiten, usw.) und die alleinige Kontrolle der Einhaltung der IT-Charta (die beispielsweise auf die Gewährleistung des Einhalts der im Unternehmen geltenden Grundsätze und Regeln in Bezug auf die Nutzung des Internets und der elektronischen Korrespondenz abzielt) fallen nicht zwangsläufig unter den Begriff des *„Schutzes der Unternehmensgüter"*. Folglich ist es nicht erlaubt, zu kontrollieren, ob der Arbeitnehmer zu privaten Zwecken im Internet surft, ob er sich an die beruflichen oder berufsständischen Regeln hält, usw., sofern diese Kontrolle ohne Bezug zum Schutz des IT-Systems oder zum Schutz vertraulicher Informationen erfolgt.

Danach analysiert die CNPD die Zulässigkeit der Verarbeitung im Hinblick auf die Grundsätze des Briefgeheimnisses und der Vertraulichkeit der Kommunikation.

Sie verpflichtet sich darüber hinaus zur Überprüfung der Verhältnismäßigkeit der Überwachung. Der Grundsatz der Verhältnismäßigkeit erfordert die Gewichtung der Überwachungsmethode im Verhältnis zu den seitens des für die Verarbeitung Verantwortlichen zu verhindern beabsichtigten konkreten Gefahren. Eine zu Überwachungszwecken erfolgende allgemeine Vorabkontrolle sämtlicher Kommunikationsdaten sowie eine Aufzeichnung sämtlicher Daten jedweder Art wird als unverhältnismäßig betrachtet.

Die seitens des Arbeitgebers diesbezüglich einzuhaltenden Bedingungen und die Art und Weise der Durchführung einer Überwachung der IT-Tools werden nachstehend ausführlich behandelt.

40 Siehe Parlamentsdokument Nr. 4735/13, S. 21.

7

7. Überwachungsarten

7.2.3.1. Verbot einer ständigen Überwachung

Die ständige Überwachung der betroffenen Personen gilt abgesehen von den gesetzlichen Ausnahmeregelungen als unverhältnismäßig. Abgesehen von den gesetzlichen Ausnahmeregelungen ist der Arbeitgeber selbst im Falle des vollständigen Verbots der Verwendung der IT-Tools zu Privatzwecken nicht zur ständigen Kontrolle der Verwendung berechtigt.

Der Grundsatz der Verhältnismäßigkeit erfordert, dass sich die seitens des Arbeitgebers eingesetzten Maßnahmen auf eine punktuelle Überwachung und auf die Einhaltung einer Abstufung bei der Steigerung der Überwachung (*„progressive Kontrollverdichtung"*) beschränken, die jedes Mal anhand vorab festgestellter Indizien und Verdachte zu rechtfertigen ist. Die schrittweise Steigerung dieser Überprüfungen darf nur im Hinblick auf die betroffenen Personen erfolgen, bei denen die punktuellen Überprüfungen Anzeichen von Missbrauch oder regelwidrigem Verhalten ergeben haben, die eine Gefahr für die Unternehmensgüter darstellen.

An dieser Stelle sei auch an die diesbezüglich gefällten bedeutenden Grundsatzurteile erinnert: **EGMR, Niemietz gegen Deutschland, 16.12.1992 und EGMR, Copland, 3. April 2007**. Diesen Rechtsprechungen zufolge fallen die Tätigkeiten des Arbeitnehmers am Arbeitsplatz und insbesondere die E-Mails und Internet-Verbindungen unter den Schutz von Artikel 8 der Europäischen Menschenrechtskonvention. Genauer gesagt *„ist das Gericht daher der Ansicht, dass die ohne Wissen der Antragstellerin erfolgende Erfassung und Speicherung von personenbezogenen Daten in Bezug auf deren Verwendung des Telefons, der E-Mails und des Internets gemäß Artikel 8 einen Eingriff in deren Recht auf Schutz ihrer Privatsphäre und ihrer Korrespondenz darstellt"*.

Grundsätzlich ist zwischen drei Bereichen der IT-Überwachung zu unterscheiden: (a) Die Überwachung der E-Mails, (b) die Überwachung der Internetnutzung und (c) die Überwachung der Datenträger und der Log-Dateien.

7.2.3.2. Kontrolle der E-Mails

Das Briefgeheimnis

Es gilt die Vermutung, dass eine elektronische Nachricht, die auf einem Computer des Arbeitgebers empfangen oder versendet wird, im Rahmen der beruflichen Tätigkeiten empfangen oder versendet wird, d.h. der Arbeitgeber selbst als Empfänger bzw. Versender betrachtet wird.

Eine solche Nachricht gilt unter den nachstehenden Voraussetzungen jedoch nicht als beruflich:

- wenn sich im Betreff der E-Mail der Vermerk *„privat"* oder *„persönlich"* befindet, oder
- wenn aus dem Betreff der E-Mail offenkundig ersichtlich wird, dass es sich um eine private E-Mail handelt, wie beispielsweise beim Betreff *„Spanienurlaub"*.

Ist dies der Fall, so darf der Arbeitgeber die persönlichen Nachrichten seiner Arbeitnehmer nicht öffnen. Tut er es doch, so verletzt er das in der Verfassung verankerte Briefgeheimnis, was nach Maßgabe des Gesetzes vom 11. August 1982 über den Schutz der Privatsphäre und des Gesetzes vom 30. Mai 2005 betreffend die spezifischen Bestimmungen bezüglich des Schutzes der Person bei der Datenverarbeitung auf dem Gebiet der elektronischen Kommunikation und betreffend die Abänderung der Artikel 88-2 und 88-4 der Strafprozessordnung einen Straftatbestand darstellt.

Der Rechtsprechung zufolge findet dieses Verbot des Lesens privater Nachrichten selbst dann Anwendung, wenn der Arbeitgeber zuvor die private Nutzung der IT-Tools untersagt hat (siehe **Kassationshof (Frankreich), Kammer für soziale Angelegenheiten, 2. Oktober 2001, Nikon**).

Das Berufungsgericht Luxemburg entschied in einer Rechtssache vom 7. April 2011 im selben Sinn wie das Nikon-Urteil: **Berufungsgericht Luxemburg, 7. April 2011, Nr. 35507 und Nr. 35651**: *„Das Gericht stellt fest, dass der Arbeitnehmer grundsätzlich und selbst während der Arbeitszeit und am Arbeitsplatz Recht auf den Schutz seiner Privatsphäre hat, was insbesondere das Briefgeheimnis umfasst, in dessen Rahmen die von ihm über ein ihm zu beruflichen Zwecken bereitgestelltes IT-Tool empfangenen E-Mails fallen. Das in Artikel 8 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten vorgesehene Briefgeheimnis findet ungeachtet des Absende- oder Empfangsortes der E-Mails auch auf die neuen Nachrichtenübertragungstechnologien Anwendung, sodass der Arbeitgeber keine konkrete und genaue Kenntnis des Inhalts der durch das Briefgeheimnis geschützten E-Mails nehmen darf."*

Auf Grundlage dieser Grundsätze entscheidet das Gericht wie folgt: *„Da der Arbeitnehmer (die E-Mails) als persönlich gekennzeichnet hat, ist der Arbeitgeber ohne Genehmigung des Arbeitnehmers nicht dazu berechtigt, sich diese E-Mails zunutze zu machen."*

An dieser Stelle ist noch anzumerken, dass der Grundsatz des Briefgeheimnisses jedoch im Rahmen einer strafrechtlichen Untersuchung oder durch einen Gerichtsbeschluss aufgehoben werden kann.

Kontrolle beruflicher E-Mails

Alle E-Mails, die nicht als *„privat"* oder *„persönlich"* gekennzeichnet sind, müssen als beruflich angesehen werden, so dass der Arbeitgeber darauf zugreifen darf.

In der ersten Kontrollphase darf der Arbeitgeber lediglich eine allgemeine Überwachung der Nachrichten durchführen. Folglich darf er Verkehrs- und Log-Daten wie z.B. Menge, Häufigkeit, Größe und Format der angehängten Dateien erheben. Diese Informationen werden kontrolliert, ohne dass der betroffene Arbeitnehmer dabei identifiziert wird.

Falls Unregelmäßigkeiten festgestellt werden, darf der Arbeitgeber in einer zweiten Phase die betroffenen Personen identifizieren und den Inhalt der beruflichen E-Mails kontrollieren.

Empfehlungen für die E-Mail-Nutzung

Um zu vermeiden, dass die Vertraulichkeit von Nachrichten persönlicher Art durch den Arbeitgeber verletzt werden könnte, empfiehlt die Nationale Kommission den Arbeitgebern die Befolgung der nachstehenden Ratschläge:

- die Arbeitnehmer sollten dazu aufgefordert werden, private Nachrichten von beruflichen Nachrichten zu unterscheiden, indem sie den privaten und persönlichen Charakter der Nachrichten im Betreff angeben und ihre Mailpartner dazu auffordern, dies ebenfalls zu tun;
- die Einrichtung eines doppelten Postfachs, um die privaten und beruflichen E-Mails voneinander zu trennen;
- die Archivierung der persönlichen Nachrichten in einem als „persönlich" gekennzeichneten Ordner.

Zugriff auf die E-Mails in Abwesenheit des Arbeitnehmers

Zur Sicherstellung des kontinuierlichen Fortgangs der Geschäftstätigkeiten des Unternehmens während der Abwesenheit (Krankheit, Urlaub, usw.) des Arbeitnehmers, erteilt die CNPD die nachstehenden Empfehlungen (nachdem der Arbeitgeber die Arbeitnehmer und die Personalvertretungsorgane darüber in Kenntnis gesetzt hat):

- das automatische Versenden einer Abwesenheits-benachrichtigung an den Absender einer E-Mail, mit Angabe der in dringenden Fällen zu kontaktierenden Personen;
- das Benennen eines Stellvertreters, der ein speziell definiertes Zugriffsrecht auf die Mail-

7

7. Überwachungsarten

box seines Arbeitskollegen besitzt: Er kann Nachrichten beruflicher Art lesen und bearbeiten, jedoch nicht Nachrichten, die als persönlich gekennzeichnet sind;

- die Weiterleitung aller eingehenden Nachrichten an einen Stellvertreter.

Jeder Arbeitnehmer muss wissen, wer sein Stellvertreter ist.

Beim endgültigen Ausscheiden des Arbeitnehmers aus dem Unternehmen wird folgendes empfohlen:

- der Arbeitnehmer, der das Unternehmen verlässt, leitet alle Dokumente beruflicher Art in Bezug auf die laufenden Akten an eine vorher festgelegte Person weiter (z.B. an seinen Vorgesetzten);
- er versichert, seinem Arbeitgeber alle Dokumente beruflicher Art ausgehändigt zu haben;
- er kann E-Mails und andere Dokumente privater Natur auf einen privaten Datenträger kopieren und sie dann aus dem Datensystem des Unternehmens entfernen;
- der Arbeitgeber verpflichtet sich, alle IT-Konten des Arbeitnehmers zu blockieren und dessen Mailbox(en) beim Ausscheiden aus dem Unternehmen zu löschen;
- Personen, die eine Nachricht an das blockierte Konto schicken, werden automatisch über die Löschung der E-Mail-Adresse in Kenntnis gesetzt und erhalten eine alternative Kontaktadresse.

Diese Regeln lehnen sich hauptsächlich an den *„Leitfaden zur Internet- und E-Mail-Überwachung am Arbeitsplatz"*[41] des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten an. Die CNPD schließt sich insbesondere bei den von ihr erteilten Genehmigungen an diese Regeln und Empfehlungen an.

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

Anwendungen im Rahmen der Rechtsprechung

Die luxemburgische Rechtsprechung ist der Ansicht, dass das Beweismittel in Ermangelung der seitens der CNPD erteilten Vorabgenehmigung unzulässig ist.

Bezirksgericht Luxemburg, 25. Mai 2012, Nr. 874/2012, (Entscheidung im Bereich des unlauteren Wettbewerbs). Der Arbeitgeber reicht als Beweismittel mehrere E-Mails ein. Seiner Ansicht nach ist er zu deren Vorlage berechtigt, da es sich nicht um private E-Mails handele. Das Gericht präzisiert, dass das Gesetz aus dem Jahr 2002 und der Artikel L.261-1 des Arbeitsgesetzbuchs sehr wohl auf berufliche E-Mails Anwendung finden und ist der Ansicht, dass im besagten Fall eine Überwachung im Sinne des Gesetzes stattgefunden hat. Das Gericht weist die E-Mails mit der Begründung zurück, dass der Arbeitgeber *„weder den Nachweis erbringt noch anführt, dass diese Überwachung in Übereinstimmung mit dem Arbeitsgesetzbuch erfolgte, was insbesondere die vorherige Inkenntnissetzung des Arbeitnehmers beinhaltet."*

Arbeitsgericht Luxemburg, 7. März 2013. In einer Entlassungsangelegenheit reicht der Arbeitgeber als Beweismittel *„eine beträchtliche Anzahl an E-Mails ein, von denen einige im Anhang des Kündigungsschreibens beigefügt sind"*, obgleich er bei der CNPD nicht die Genehmigung für eine Überwachung der E-Mails beantragt hat. Das Gericht ist der Ansicht, dass: *„die nicht nur gelegentlich erfolgte Aufzeichnung dieser Daten und die daraus erfolgte Bestimmung des Verhaltens des Arbeitnehmers als Überwachung im Sinne von Artikel 2 des abgeänderten Gesetzes vom 2. August 2002 zum Schutz personenbezogener Daten bei der Datenverarbeitung zu betrachten ist. Demnach kann die Verarbeitung von personenbezogenen Daten zu Überwachungszwecken am Arbeitsplatz ausschließlich nach Maßgabe des vorgenannten Gesetzes und nach Maßgabe der Bestimmungen aus Artikel L.261-1 des Arbeitsgesetzbuchs erfolgen."* Folglich entfernte das Gericht die betreffenden E-Mails aus der Verhandlung.

7.2.3.3. Kontrolle der Internetnutzung

Die meisten Arbeitgeber stellen ihren Arbeitnehmern am Arbeitsplatz einen Internetzugang für berufliche Zwecke bereit.

Demnach kann der Arbeitgeber die Bedingungen und Einschränkungen für die private Internetnutzung festlegen, deren Kontrolle möglich sein muss. Dies wurde durch die französische Rechtsprechung bestätigt: **Kassationshof (Frankreich), Kammer für soziale Angelegenheiten, 9. Juli 2008**[42]. Neben der Pflicht zur Beantragung einer Genehmigung bei der CNPD, muss der Arbeitgeber die Arbeitnehmer aber auch vorab unmissverständlich darüber in Kenntnis setzen, durch welche Mittel die Kontrolle erfolgt und welchen Modalitäten sie unterliegt. Andernfalls würde es sich um eine heimliche Kontrolle handeln, die ohne Wissen der Arbeitnehmer erfolgt.

Er darf keinen bestimmten, identifizierbaren Arbeitnehmer überwachen, ohne zuvor eine allgemeine und nicht personalisierte Überwachung durchgeführt zu haben. So kann er beispielsweise eine allgemeine Liste der über einen bestimmten Zeitraum besuchten Webseiten aufstellen, aus der die Identität der Webseitenbesucher nicht hervorgeht. Ergeben sich daraus Hinweise in Bezug auf eine für das Unternehmen schädliche Internetnutzung (z.B. durch eine außergewöhnlich lange Nutzungsdauer oder durch das Besuchen verdächtiger Websites), so kann der Arbeitgeber angemessene Kontrollmaßnahmen ergreifen und in einer zweiten Phase eine individualisierte Überwachung durchführen.

Angesichts der Gefahr, das Datensystem über verdächtige Websites mit Viren zu infizieren, empfiehlt die Nationale Kommission den Einsatz vorbeugender Schutzmaßnahmen wie z.B. die Herausfilterung nicht erlaubter Websites oder das Verbot von Software-Downloads oder der Verbindung zu Diskussionsforen.

7.2.3.4. Kontrolle der Datenträger und der Log-Dateien

Allgemein werden alle seitens eines Arbeitnehmers erstellten Dokumente und Dateien als beruflich betrachtet. Der Arbeitnehmer kann jedoch in einem vernünftigen Rahmen Dokumente und Dateien erstellen, die er als persönlich kennzeichnet (dieser Grundsatz wurde seitens der Rechtsprechung bestätigt). Nach Maßgabe des Urteils Cathnet-Science, **Kassationshof (Frankreich), Kammer für soziale Angelegenheiten, 17. Mai 2005**, darf der Arbeitgeber die auf der Festplatte des Computers eines Arbeitnehmer enthaltenen und von diesem als persönlich gekennzeichneten Akten in dessen Abwesenheit oder ohne dessen „ordnungsgemäße Einberufung" nicht öffnen.

Auch hier darf die Überwachung der Datenträger und der Log-Dateien keine Individualisierung beinhalten, sondern muss in Bezug auf Zeitabstand und Volumen der kontrollierten Daten abgestuft werden. Anders ausgedrückt ist der Arbeitgeber nicht zur unverzüglichen Durchführung einer individuellen Kontrolle berechtigt, ohne zuvor eine allgemeine Kontrolle durchgeführt zu haben, bei der Unregelmäßigkeiten festgestellt wurden.

Dateien oder Dokumente, die als privat gekennzeichnet sind, dürfen seitens des Arbeitgebers nur in Anwesenheit des betroffenen Mitarbeiters geöffnet werden. Dieser muss dabei die Möglichkeit haben, der Öffnung einer privaten Datei zu widersprechen und muss bei der Kontrolle über diese Möglichkeit informiert werden.

Die CNPD empfiehlt demnach, dass der Arbeitgeber Maßnahmen ergreift, die sicherstellen, dass die elek-

42 „Es wird angenommen, dass der seitens eines Arbeitnehmers während seiner Arbeitszeit über das ihm seitens seines Arbeitgebers zur Verfügung gestellte IT-Tool erfolgte Aufruf von Webseiten im Rahmen seiner beruflichen Tätigkeit erfolgt, sodass der Arbeitgeber diese in seiner Abwesenheit zum Zwecke ihrer Identifizierung durchsuchen kann".

7

7. Überwachungsarten

tronischen Dokumente des Unternehmens während der Abwesenheit des Mitarbeiters zugänglich sind, ohne dass dabei die „persönlichen oder privaten" Ordner des Arbeitnehmers geöffnet werden müssen.

Schließlich wird empfohlen, dass der Arbeitnehmer am Ende seines Arbeitsverhältnisses eine Kopie der in seinem privaten Ordner gespeicherten Dokumente erhält und darüber hinaus die Möglichkeit hat, seine persönlichen Ordner aus dem Datensystem zu entfernen, ggf. in Anwesenheit eines Vertreters des Arbeitgebers.

Anwendungen im Rahmen der Rechtsprechung

Berufungsgericht Luxemburg, 3. März 2011, Nr. 35462: Ein Arbeitnehmer empfängt über seine private E-Mail-Adresse ein Dokument mit der Bezeichnung „brainstorming.doc", das auf der Festplatte seines für berufliche Zwecke verwendeten Computers gespeichert wird. Das besagte Dokument wird trotz seiner Löschung danach seitens des Arbeitgebers auf dem Computer „wiederhergestellt". Der Arbeitnehmer ist der Ansicht, dass der Arbeitgeber gegen das Briefgeheimnis verstoßen hat. Das Gericht erinnert unter Verweis auf die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte und auf das Nikon-Urteil daran, dass *„der Arbeitnehmer selbst während seiner Arbeitszeit und an seinem Arbeitsplatz Recht auf den Schutz der Vertraulichkeit seiner Privatsphäre hat und dies insbesondere das Briefgeheimnis betrifft"*. Das Gericht ist jedoch der Ansicht, dass die Bezeichnung des Dokuments *„nicht a priori auf einen privaten Charakter schließen ließ"* und es unbegründet sei, das Dokument außer Acht zu lassen, d.h. das Dokument ist als Beweismittel zulässig.

7.2.3.5. Pflicht zur Information der betroffenen Arbeitnehmer

Der Arbeitgeber muss seine Arbeitnehmer darüber in Kenntnis setzen, inwieweit er die zu persönlichen Zwecken erfolgende Nutzung der IT-Tools und der zur Verfügung gestellten Geräte gestattet und welche Methoden er zur Kontrolle dieser Geräte einsetzt. Anders ausgedrückt muss er die Arbeitnehmer davon unterrichten, in welchem Maße er ihnen die Nutzung von E-Mails und/oder das Surfen im Internet und/oder die Erstellung und Speicherung persönlicher Dateien gestattet.

Diesbezüglich sollen unter anderem die nachstehenden Informationen gegeben werden betreffend:

- die Nutzung der IT-Infrastruktur zu privaten Zwecken (Nutzungszeiträume und Nutzungsdauer, Art und Weise der Speicherung der Daten auf der Festplatte,...);
- die Gründe und Zwecke der Kontrolle, die Art der dabei erhobenen Daten, das Ausmaß und die Umstände der Kontrollen; die Personen, denen die erhobenen Daten zugänglich sind;
- den Einsatz von Tools, die bestimme Webseiten und/oder Ketten-E-Mails und/oder übergroße Dateien blockieren;
- die Art und Weise der Erhebung und der Nutzung der aus der Überwachung gewonnenen Daten;
- die Personen, die zur Nutzung der aus der Überwachung gewonnenen Daten berechtigt sind und die Umstände, unter denen eine solche Nutzung gestattet ist;
- die Speicherdauer der aus der Überwachung gewonnenen Daten;
- die Entscheidungen, die der Arbeitgeber bei einer Kontrolle fällen könnte;
- die Rolle der Arbeitnehmervertreter bei der Umsetzung der Überwachungspolitik;
- die Modalitäten des Zugriffsrechts der Arbeitnehmer auf die sie betreffenden Daten.

Im Hinblick auf Transparenz und Aufrichtigkeit in den Arbeitsbeziehungen empfiehlt die CNPD den Arbeitgebern die Annahme einer Charta, einer Geschäfts-

ordnung oder anderer Dokumente in Bezug auf die Nutzung und die Kontrollmethoden der den Arbeitnehmern zur Verfügung gestellten IT-Tools.

Selbstverständlich sind auch externe Arbeiter und Mitarbeiter, deren Verwendung der IT-Tools und E-Mails überwacht werden könnte, vorab darüber in Kenntnis zu setzen.

7.2.3.6. Begrenzte Speicherdauer

Für die Überwachung der IT-Tools ist die CNPD in der Regel der Ansicht, dass eine sechsmonatige Speicherdauer der aus der Überwachung gewonnenen Daten ausreicht.

Im Rahmen der Weitergabe der Daten an die zuständigen Justizbehörden können die Daten jedoch länger als oben genannt gespeichert werden.

Die oben genannten maximalen Speicherzeiträume gelten nicht für Geschäfts- und Buchführungsunterlagen, die bis zum Ablauf der geltenden Verjährungsfristen gespeichert werden können.

7.2.3.7. Rolle der Systemadministratoren / Netzwerkadministratoren

Die Administratoren, denen die Gewährleistung des ordnungsgemäßen Betriebs und der Sicherheit der IT-Netze und –Systeme obliegt, haben aufgrund ihrer Tätigkeit Zugriff auf sämtliche Nutzerinformationen (E-Mails, Internetverbindungen, „Log"- oder Protokolldateien, usw.), einschließlich derer, die auf der Festplatte des Arbeitsplatzes aufgezeichnet sind.

Demnach müssen sie einer verstärkten Verpflichtung zur Wahrung des Betriebsgeheimnisses oder der beruflichen Schweigepflicht unterliegen. Allgemein billigt und übernimmt die CNPD im Rahmen ihrer Genehmigungen bestimmte seitens der „Commision Nationale de l'informatique et des libertés" (CNIL) ausgearbeitete Anmerkungen und Anforderungen und ist der Auffassung, dass: *„der Zugriff auf die seitens der Arbeitnehmer in ihrem IT-Umfeld aufgezeichneten Daten – die zuweilen privater Natur sind – ausschließlich dann gerechtfertigt ist, wenn der ordnungsgemäße Betrieb der IT-Systeme nicht durch andere und weniger stark in die Privatsphäre eindringende Mittel gewährleistet werden kann.*

Darüber hinaus können die Informationen, von denen die Netzwerk- und Systemadministratoren in Ausübung ihrer Tätigkeit Kenntnis erlangen können, weder eigenständig noch auf Anweisung eines Vorgesetzten zu anderen als den mit dem ordnungsgemäßen Betrieb und der Sicherheit der Anwendungen verbundenen Zwecken genutzt werden.

Ebenso ist es den Netzwerk- und Systemadministratoren, die im Allgemeinen dem Betriebsgeheimnis oder der beruflichen Schweigepflicht unterliegen, untersagt, Informationen zu verbreiten, in deren Kenntnis sie im Rahmen der Ausübung ihrer Tätigkeit gelangt sind, und insbesondere, sofern diese Informationen dem Briefgeheimnis unterliegen oder Teil der Privatsphäre der Benutzer sind und weder den ordnungsgemäßen technischen Betrieb und die Sicherheit der Anwendungen noch die Interessen des Unternehmens gefährden. Sie sind abgesehen von einer diesbezüglichen gesetzlichen Sonderbestimmung auch nicht zu deren Offenlegung verpflichtet.[43] "

7.2.3.8. Protokolldateien

Die der Identifizierung und Aufzeichnung aller Verbindungen oder Verbindungsversuche zu einem automatisierten Informationssystem dienenden Protokolldateien kommen der Sicherheit und Vertraulichkeit der personenbezogenen Daten zugute. Sie dürfen unbefugten Dritten weder zugänglich sein noch zu anderen als den ihre Verarbeitung rechtfertigenden Zwecken genutzt werden. Ihre Hauptaufgabe besteht nicht in der Kontrolle der Benutzer.

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

7

7. Überwachungsarten

Da die Protokolldateien der Sicherheit und der Vertraulichkeit dienen, sind sie nicht als Verarbeitung zu Überwachungszwecken zu betrachten.

Der Einsatz einer Software zur Analyse der verschiedenen Protokolle (Anwendungen und Systeme), die die Erhebung von arbeitsplatzspezifischen Informationen zur Kontrolle der Tätigkeiten des Benutzers ermöglicht, ist hingegen als Verarbeitung zu Überwachungszwecken mit allen damit verbundenen Folgen zu betrachten, wie der Erfordernis einer Genehmigung seitens der Nationalen Kommission, der Begrenzung der Maßnahmen auf das Zulässigkeitskriterium des Schutzes der Unternehmensgüter und der Verhältnismäßigkeit der möglichen Kontrollen.

7.3. Aufzeichnung von Telefongesprächen

Ein Arbeitgeber kann im Rahmen seiner Geschäftstätigkeit zur Aufzeichnung der Telefongespräche seiner Arbeitnehmer und ihrer Gesprächspartner veranlasst sein.

Diese Überwachungsmaßnahme ist insbesondere im Finanzsektor gängige Praxis, wo die Fachkräfte die Telefongespräche aufzeichnen, um sich einen Nachweis über die Geschäftstransaktionen (z.B. Börsengeschäfte) zu verschaffen. Wenngleich diese Zweckbestimmung bis 2007 die einzige war, für die die Verarbeitung genehmigt werden konnte, hat der Gesetzgeber seither den Anwendungsbereich der Aufzeichnungen von elektronischen Kommunikationen allgemein und von Telefongesprächen im Besonderen durch Hinzufügung der Zweckbestimmung des Nachweises *„jedweder sonstigen Geschäftskommunikation“* erweitert, womit er beispielsweise auf die Aufzeichnung von Telefongesprächen der *„Call Center“*, der *„Helpdesks“*, der Kundendienste, usw. abzielt.

7.3.1. Welche Zielsetzungen kann der Arbeitgeber verfolgen?

Im Rahmen des Alltagsgeschäfts von Banken, Finanzinstituten und bestimmten anderen Handelsgesellschaften werden Telefongespräche im Allgemeinen aus den nachstehenden Zwecken aufgezeichnet:

- die Erfordernis eines Nachweises der Geschäftstransaktionen oder der Geschäftskommunikationen für den Streitfall,
- der Erwerb von Daten über Verhandlungen, Arbeitsvorgänge, Beschlüsse, Transaktionen, usw.,
- die Überprüfung der telefonisch vereinbarten Geschäftsverpflichtungen,
- die Bestätigung der Einzelheiten eines Börsenauftrags/einer Anweisung (Verkauf, Kauf, Zeichnung, Lieferung, usw.),
- das erneute Anhören von Anweisungen,
- die Beseitigung von Missverständnissen.

7.3.2. In welchen Fällen können Telefongespräche aufgezeichnet werden?

Der Grundsatz der Vertraulichkeit der Kommunikationen wird in zahlreichen nationalen und internationalen Rechtstexten untermauert:

- Artikel 28 der Verfassung: *„Das Briefgeheimnis ist unverletzlich (...)“*,
- Artikel 8 der Europäischen Menschenrechtskonvention vom 4. November 1950: *„Jede Person hat das Recht auf Achtung ihres Privat-*

und Familienlebens, ihrer Wohnung und ihrer Korrespondenz",

- die am 7. Dezember 2000 in Nizza verkündete Charta der Grundrechte der Europäischen Union enthält dieselbe Formulierung, ersetzt jedoch den Begriff *„Korrespondenz"* durch den Begriff *„Kommunikation"*,
- das Gesetz vom 11. August 1982 über den Schutz der Privatsphäre,
- das abgeänderte Gesetz vom 2. August 2002 zum Schutz personenbezogener Daten bei der Datenverarbeitung, das vorbehaltlich restriktiver Bedingungen die Möglichkeit der Verarbeitung personenbezogener Daten zu Überwachungszwecken vorsieht, darunter unter anderem auch die Aufzeichnung von Telefongesprächen,
- das abgeänderte Gesetz vom 30. Mai 2005 betreffend die spezifischen Bestimmungen zum Schutz personenbezogener Daten bei der Datenverarbeitung auf dem Gebiet der elektronischen Kommunikation (zur Umsetzung der als *„Privatsphäre und elektronische Kommunikation"* bezeichneten Richtlinie 2002/58/EG in innerstaatliches luxemburgisches Recht), das die Möglichkeit zur Aufzeichnung von Kommunikationen vorsieht, sofern diese *„im Rahmen der zulässigen geschäftlichen Nutzung erfolgen, um den Nachweis für eine geschäftliche Transaktion oder jedwede sonstige geschäftliche Kommunikation zu liefern"*.

Die nationalen und internationalen Gesetzestexte zeugen demnach von der Bedeutung der Vertraulichkeit der Kommunikationen. Überdies präzisierte die Rechtsprechung des EGMR, dass Telefonanrufe zweifelsohne unter den Begriff der *„Privatsphäre"* und der *„Korrespondenz"* fallen (siehe **EGMR, Halford gegen das Vereinigte Königreich, 25. Juni 1997, und EGMR, Copland gegen das Vereinigte Königreich, 3. April 2007**). Obgleich der Gesetzgeber eine Überwachung mittels der Aufzeichnung von Telefongesprächen ermöglicht hat, so unterstellt er diese restriktiven Bedingungen, die die Interessen der betroffenen Personen bezüglich des Schutzes ihrer Privatsphäre mit den Interessen der für die Verarbeitung Verantwortlichen in Einklang bringen.

Im Falle des Auftretens von Klagen oder Streitigkeiten können die Aufzeichnungen von Telefongesprächen am Arbeitsplatz demnach ausschließlich als Nachweise für eine Geschäftstransaktion oder eine „sonstige" Geschäftskommunikation dienen. *Nicht erlaubt sind demnach* Aufzeichnungen von Privatgesprächen sowie Aufzeichnungen, deren Zwecke nicht unter die gesetzlichen Bestimmungen fallen, wie beispielsweise:

- die Kontrolle der beruflichen Leistungen der Arbeitnehmer,
- die Verwendung der erhobenen Daten zur Beurteilung der Arbeitnehmer,
- die Kontrolle der Qualität der Telefongespräche.

7.3.3. Die an Bedingungen und Empfehlungen geknüpfte Vorabgenehmigung der CNPD

In jeder ihrer Genehmigungen setzt die CNPD eine Reihe von Bedingungen und Erfordernissen fest, die sich aus den allgemeinen Grundsätzen der Gesetzgebung über den Datenschutz ergeben.

So untersucht die CNPD von Fall zu Fall, ob die seitens des Arbeitgebers verfolgten Zielsetzungen mit den gesetzlich vorgesehenen zulässigen Fällen übereinstimmen. Überdies überprüft sie die Notwendigkeit und die Verhältnismäßigkeit der telefonischen Aufzeichnungen.

7

7. Überwachungsarten

7.3.3.1. Verbot der systematischen Aufzeichnung aller Telefonanschlüsse

Genehmigt wird lediglich die Aufzeichnung der Telefonanschlüsse der seitens des Arbeitgebers zuvor festgesetzten Abteilungen, die für die Geschäftstätigkeit des Unternehmens bedeutend sind und von denen aus Geschäftskommunikationen getätigt werden (z.B.: Trading Room, Abteilung Private Banking, Fondsmanagement, Helpdesk, usw.). Die CNPD ist der Ansicht, dass die systematische Aufzeichnung der von allen Telefonanschlüssen des Unternehmens getätigten Gespräche in Bezug auf die Zweckbestimmung, die im Erhalt des Nachweises über eine Transaktion oder eine Geschäftskommunikation besteht, unverhältnismäßig ist. Die Überwachung der Telefonanschlüsse der Abteilungen, die von vornherein nicht unter diese Zweckbestimmung fallen, wird im Allgemeinen nicht genehmigt.

7.3.3.2. Bereitstellung einer separaten, nicht überwachten Leitung

Innerhalb der genehmigten Abteilungen muss der Arbeitgeber den Arbeitnehmern und den externen Gesprächspartnern eine nicht überwachte Telefonleitung zur Verfügung stellen, damit diese nicht aufgezeichnete Telefongespräche zu privaten/persönlichen Zwecken führen können.

7.3.3.3. Information der Arbeitnehmer und Dritten

Die Überwachung von Telefongesprächen betrifft sowohl die Arbeitnehmer des für die Verarbeitung Verantwortlichen als auch deren Gesprächspartner. Diesbezüglich unterscheidet die CNPD zwischen beruflichen Gesprächspartnern, die aus einem Sektor stammen, in dem die Aufzeichnung von Telefongesprächen zur zulässigen Berufspraxis gehört (wie beispielsweise die Akteure des Finanzsektors, wie Börsenmakler) und Geschäftspartnern, bei denen es sich um Privatpersonen handelt (z.B. die Kunden).

Daher variieren die Pflichten des für die Verarbeitung Verantwortlichen in Abhängigkeit von der jeweiligen Personenkategorie:

- **Was die Arbeitnehmer betrifft**, so müssen diese obligatorisch über die Überwachung informiert werden (ebenso wie gegebenenfalls deren Vertretungsorgane). Diese Informationspflicht ergibt sich nicht nur aus den spezifischen Bestimmungen des abgeänderten Gesetzes vom 30. Mai 2005, sondern auch aus den allgemeinen Bestimmungen des abgeänderten Gesetzes vom 2. August 2002 in Bezug auf die Überwachung der Arbeitnehmer.

  Hierbei handelt es sich um eine Vorabinformationspflicht *„der an den Transaktionen beteiligten Parteien"* (durch vorherige Mitteilung oder spezielle Vereinbarung), ohne die die Aufzeichnung als Beweismittel vor einem Gericht gegebenenfalls als gegenstandslos betrachtet werden kann. Siehe diesbezüglich: (**LU**) **Berufungsgericht Luxemburg, 24. Oktober 2002, Nr. 25235 des Gerichtsverzeichnisses, BIJ 2002, S.39** *„Es gilt festzustellen, dass das Arbeitsgericht mit Recht und aus den seitens des Berufungsgerichts übernommenen Gründen, die ohne Wissen einer der Parteien durchgeführte Tonbandaufzeichnung als Beweismittel zurückgewiesen hat".*
- **Was nicht berufliche Gesprächspartner betrifft** (wie beispielsweise private Kunden), so führte das abgeänderte Gesetz vom 30. Mai 2005 eine Bestimmung ein (Artikel 4, Absatz 3, Buchstabe d), die vorsieht, dass der für die Verarbeitung Verantwortliche ausschließlich in dem Fall nicht mehr dazu verpflichtet ist, zur Durchführung der Aufzeichnung die Einwilligung der an der Kommunikation beteiligten Parteien einzuholen, in dem diese

Aufzeichnung *„im Rahmen der zulässigen Berufspraxis erfolgt, um den Nachweis über einen Geschäftsvorgang oder jedwede sonstige Geschäftskommunikation zu liefern"*. Dieselbe Bestimmung des Gesetzes unterstellt den für die Verarbeitung Verantwortlichen hingegen ganz eindeutig der Vorabinformation der beteiligten Parteien über die Bedingungen der Gesprächsaufzeichnung, die Gründe, aus denen die Gespräche aufgezeichnet werden sowie die maximale Speicherdauer der Daten.

Um dritte und nicht berufliche Gesprächspartner (insbesondere Kunden) hinreichend klar auf die Bedingungen der Gesprächsaufzeichnung hinzuweisen, ist die CNPD daher der Ansicht, dass diese Vorabinformation durch die Unterzeichnung einer speziellen Vereinbarung in Bezug auf die Verwendung des angebotenen Telefondienstes erfolgen muss (und nicht in den allgemeinen Bedingungen „untergehen" darf). In diesem Fall muss der für die Verarbeitung Verantwortliche auch sämtliche erforderlichen organisatorischen und technischen Maßnahmen ergreifen, um zu verhindern, dass Gespräche aufgezeichnet werden, die nichts mit Geschäftsvorgängen oder Geschäftskommunikationen zu tun haben oder mit Personen geführt werden, bei denen es sich nicht um Kunden oder bei denen es sich um potenzielle Kunden handelt. Wenn diese beiden Bedingungen nicht gleichzeitig eingehalten werden können, hält es die CNPD für notwendig, dass die Drittgesprächspartner bei jedem aufgezeichneten Telefongespräch durch die Übermittlung einer automatischen oder nicht automatischen Nachricht zu Beginn des Anrufs speziell auf die Aufzeichnung hingewiesen werden.

- **Was berufliche Gesprächspartner betrifft, die aus einem Sektor stammen, in dem die Aufzeichnung von Telefongesprächen zur zulässigen Berufspraxis gehört** (wie bei Finanzmaklern, Fondsmanagern, Angestellten anderer Banken, usw.), so ist eine Vorabinformation zu Beginn jedes Anrufs nicht erforderlich.

7.3.3.4. Begrenzte Speicherdauer

Nach Ansicht der CNPD kann der für die Verarbeitung Verantwortliche die aus den Aufzeichnungen der Telefongespräche gewonnenen Daten über einen Zeitraum von maximal zehn Jahren ab dem Aufzeichnungsdatum speichern. Dieser Zeitraum deckt sich mit der zehnjährigen Verjährungsfrist für Geschäftsvorgänge und Geschäftskommunikationen, für die die Telefonaufzeichnungen als Nachweis dienen können.

7.4. Die biometrischen Systeme

Biometrische Daten können wie folgt definiert werden: *„Biologische Eigenschaften, Verhaltensweisen, physiologische Merkmale, Gesichtszüge oder reproduzierbare Handlungen, wobei diese Merkmale und/oder Handlungen für die betreffende Person spezifisch und messbar sind, auch wenn die in der Praxis angewandten Modelle für ihre technische Messung in gewissem Umfang auf Wahrscheinlic keiten beruhen"*[44]. Beispiele für biometrische Daten sind Fingerabdrücke, die Venenstruktur der Finger, aber auch der Tastenanschlag am Klavier.

Biometrische Daten sind keine personenbezogenen Daten im üblichen Sinne. Sie werden weder von Dritten zugewiesen noch von der Person selbst gewählt. Sie ermöglichen die endgültige und zweifellose Identifizierung einer Person anhand bestimmter einzigartiger Eigenschaften ihres Körpers.

44 Stellungnahme 4/2007 vom 20. Juni 2007 zum Begriff „personenbezogene Daten" der Artikel-29-Datenschutzgruppe, S. 9, verfügbar unter nachstehender Adresse: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_fr.pdf

7

7. Überwachungsarten

Der Missbrauch oder die Veruntreuung dieser Daten kann demnach schwerwiegende Folgen haben[45].

Da die biometrischen Daten die unabänderliche Identifizierung einer Person über deren physiologische Merkmale oder Verhaltensweisen ermöglichen, möchten einige Arbeitgeber, wie in Punkt 7.4.1. dargelegt, auf Verarbeitungen zurückgreifen können, die biometrische Daten enthalten.

Aus eben diesem Grund beinhalten Systeme, die biometrische Daten einsetzen, weitaus höhere Risiken als beispielsweise ein (nicht biometrisches) Videoüberwachungssystem. Es hat sich gezeigt, dass die Vervielfältigung biometrischer Daten wie Fingerabdrücke ohne Wissen der betroffenen Personen sehr einfach sein und schlichtweg über die von diesen hinterlassenen Spuren erfolgen kann (beispielsweise auf einem Glas)! Im Gegensatz zu beispielsweise einem Passwort, kann eine biometrische Angabe niemals zurückgesetzt werden.

Daher unterliegen Verarbeitungen, die biometrische Daten enthalten, die zur Überprüfung der Identität von Personen erforderlich sind, gemäß Artikel 14, Absatz (1), Buchstabe (f) des Gesetzes vom 2. August 2002 der Vorabgenehmigung der Nationalen Kommission. In nachstehendem Punkt 7.4.3. stellen wir die Bedingungen vor, unter denen die Nationale Kommission derartige Datenverarbeitungen genehmigt oder ablehnt.

7.4.1. Welche Zielsetzungen kann der Arbeitgeber verfolgen?

Durch den Rückgriff auf biometrische Systeme kann der Arbeitgeber die Identität von Personen überprüfen. Diese Zielsetzung kann zwar auch über andere Verfahren wie den Einsatz von Firmenausweisen oder Passwörtern erfüllt werden, doch während Firmenausweise und Passwörter sehr leicht ausgewechselt oder vertauscht werden können, ermöglichen die biometrischen Systeme die unmissverständliche Identifizierung der Person, die einen bestimmten Raum betreten möchte. Die Verschärfung der Sicherheitsmaßnahmen für den Zutritt zu bestimmten Räumen oder IT-Servern, stellen demnach Beispiele für die Zweckbestimmungen dar, die der Arbeitgeber geltend machen kann, wenn er auf biometrische Systeme zurückgreifen möchte.

7.4.2. In welchen Fällen können biometrische Systeme eingesetzt werden?

Der Arbeitgeber muss mindestens eine der nachstehenden Zulässigkeitsbedingungen aus Artikel L.261-1(1) des Arbeitsgesetzbuchs geltend machen:

- die Kontrolle der Arbeitszeiten;
- den Schutz der Unternehmensgüter;
- die Sicherheit und die Gesundheit der Arbeitnehmer.

Kontrolle der Arbeitszeiten

Der Arbeitgeber beabsichtigt beispielsweise die Einrichtung eines Stechuhrsystems mittels eines biometrischen Lesegeräts, das gegenüber den Firmenausweisen den Vorteil aufweist, dass es bestimmte Missbräuche zu vermeiden ermöglicht, die im Austausch der Firmenausweise unter den Arbeitskollegen zur Änderung der Uhrzeit des Betretens und Verlassens der Räumlichkeiten des Arbeitgebers bestehen.

45 „Biometrie: Die Genehmigung der CNIL erfordernde sensible Geräte", Artikel unter der nachstehenden Adresse verfügbar: http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/biometrie-des-dispositifs-sensibles-soumis-a-autorisation-de-la-cnil/

Schutz der Unternehmensgüter

Der Arbeitgeber möchte den Schutz bestimmter Bereiche seiner Räumlichkeiten verstärken, die seiner Ansicht nach besonders empfindliche Güter oder Daten enthalten, wie beispielsweise der Server-Raum. Auf diese Weise möchte er sicherstellen, dass diesen Raum lediglich die zutrittsberechtigten Beschäftigten betreten können – eine Garantie, die unter Einsatz anderer Zutrittskontrollmaßnahmen weniger stark ausgeprägt ist.

Sicherheit und Gesundheit der Arbeitnehmer

Beispielsweise möchte der Arbeitgeber den Zutritt zu einem Raum mit gesundheitsgefährdenden Erzeugnissen (Viren, Chemikalien, usw.) beschränken, deren äußerst vorsichtige Handhabung ausschließlich berechtigten Personen innerhalb eines Labors gestattet ist.

7.4.3. Die Vorabgenehmigung der CNPD

Da biometrische Daten höhere Risiken in Bezug auf den Datenschutz aufweisen, ist die Nationale Kommission der Ansicht, dass ein Arbeitgeber nach Maßgabe des Grundsatzes der Verhältnismäßigkeit nur dann auf ein biometrisches System zurückgreifen darf, wenn dies zur Erfüllung seiner Zwecke absolut erforderlich ist, und nicht nur, weil diese Systeme für den Arbeitgeber schlichtweg „nützlicher", „zweckmäßiger" oder „praktischer" als die traditionelleren Systeme wie Passwörter oder Zutrittsausweise sind.

Die Verhältnismäßigkeit beinhaltet, dass der Arbeitgeber die Datenverarbeitung auf Daten beschränken muss, die im Hinblick auf die zu erzielenden Zwecke angemessen und zutreffend sind und nicht darüber hinausgehen. Zur Überprüfung der Einhaltung dieser Verhältnismäßigkeitsbedingung unterscheidet die CNPD einerseits zwischen Systemen, die biometrische Daten einsetzen, die Spuren hinterlassen und Systemen, die biometrische Daten einsetzen, die keine Spuren hinterlassen, und andererseits zwischen Systemen, die biometrischen Daten in einer zentralen Datenbank speichern und Systemen, die diese Daten lediglich dezentral speichern, wie beispielsweise in einem Firmenausweis.

Biometrische Daten, die Spuren hinterlassen, und biometrische Daten, die keine Spuren hinterlassen

Biometrische Daten, die Spuren hinterlassen, wie beispielsweise Fingerabdrücke, gelten als potentiell größter Eingriff in die persönlichen Freiheiten, da die Spuren ohne Wissen der betroffenen Personen aufgezeichnet und vervielfältigt werden können. Die Tatsache, dass die biometrischen Daten über einen Algorithmus in einen Datensatz (den sogenannten Template) umgewandelt werden, beseitigt diese Gefahr nicht.

Biometrische Daten, die keine Spuren hinterlassen, wie beispielsweise die Form der Hand, die Netzhaut, die Venenstruktur einer Hand oder eines Fingers, stellen nicht dieselben Gefahren dar wie biometrische Daten, die Spuren hinterlassen.

Zentral oder dezentral gespeicherte biometrische Daten

Biometrische Daten, die in einer zentralen Datenbank gespeichert werden, auf die auch andere Personen als der Arbeitgeber selbst Zugriff haben, stellen größere Gefahren dar als biometrische Daten, die auf einem einzelnen Datenträger (beispielsweise auf einem Firmenausweis oder einer Magnetkarte) gespeichert werden, über den der Arbeitgeber die alleinige Kontrolle hat.

Auf Grundlage dieser doppelten Unterscheidung genehmigt die CNPD zum gegenwärtigen Stand der eingesetzten Technologien die nachstehenden Systeme:

- Systeme, die biometrische Daten enthalten, die keine Spuren hinterlassen (beispielsweise die Form der Hand, die Venenstruktur), un-

7

7. Überwachungsarten

geachtet dessen, ob die biometrischen Daten zentral oder dezentral gespeichert werden. Diese Daten können nämlich nicht ohne Wissen der betroffenen Personen verwendet werden.

- Die Verarbeitung biometrischer Daten, die dezentral auf einem beweglichen Träger gespeichert sind (ein Firmenausweis, eine Magnetkarte), ungeachtet dessen, ob sie Spuren hinterlassen (wie beispielsweise Fingerabdrücke) oder nicht.

Die CNPD lehnt hingegen grundsätzlich Systeme ab, die biometrische Daten enthalten, die Spuren hinterlassen (wie Fingerabdrücke), wenn diese Daten oder die Templates in einer zentralen Datenbank gespeichert werden. In absoluten Ausnahmefällen können diese Verarbeitungen hingegen genehmigt werden, sofern der Antragsteller zwingende Gründe für die Sicherheit oder den Schutz der in den zu schützenden Räumlichkeiten durchgeführten Geschäftstätigkeit nachweist, und der Zugriff auf eine sehr begrenzte Anzahl von Personen beschränkt ist, die zum Betreten eines abgegrenzten Bereichs befugt sind, der ein wichtiges Schutzobjekt darstellt oder beinhaltet, das über das alleinige Interesse des für die Verarbeitung Verantwortlichen hinausgeht. Diese Fälle kommen in der Praxis jedoch sehr selten vor.

Allgemein empfiehlt die CNPD die Wahl von Systemen, die mit biometrischen Daten arbeiten, die keine Spuren hinterlassen (wie beispielsweise oben beschrieben die Form der Hand oder die Venenstruktur) und ebenso zuverlässig sind wie die Systeme mit Fingerabdrücken und die verfolgten Zwecke ebenfalls erfüllen.

Begrenzte Speicherdauer der Daten

Das Datenschutzgesetz sieht vor, dass die Daten nicht länger gespeichert werden dürfen als über den Zeitraum, der für die Erfüllung der Zwecke erforderlich ist, für die die Daten erfasst wurden. Eine begrenzte Speicherdauer der Daten stellt eine zusätzliche Garantie zur Vermeidung möglicher Zweckentfremdungen dar.

Was die biometrischen Daten betrifft, so dürfen diese nach Ansicht der CNPD nur so lange gespeichert werden, wie die betroffene Person zum Zutritt zu den abgegrenzten Bereichen befugt ist.

Darüber hinaus ist die Nationale Kommission der Ansicht, dass der Antragsteller die Daten in Bezug auf die Zutrittskontrollen, d.h. den chronologischen Überblick über die erfolgten Zugänge, über einen Zeitraum von maximal drei Monaten ab deren Aufzeichnung speichern darf.

Abschließend dürfen die Daten in Bezug auf die Kontrolle der Arbeitszeiten bei Arbeitnehmern und diesen gleichgestellten Personen nicht länger als drei Jahre und bei Angestellten des öffentlichen Dienstes nicht länger als fünf Jahre gespeichert werden.

Im Falle eines Zwischenfalls müssen die Daten in Bezug auf die Zutrittskontrollen oder die Kontrolle der Arbeitszeiten bei deren Weiterleitung an die zuständigen Justizbehörden zur Feststellung oder Verfolgung einer Straftat nicht nach Ablauf eines Zeitraums von drei Monaten bzw. drei oder fünf Jahren vernichtet werden.

7.5. Geolokalisierungsgeräte

Die „traditionelleren" Systeme zur Geolokalisierung der seitens der Arbeitnehmer verwendeten Dienstfahrzeuge werden immer häufiger durch tragbare Geolokalisierungsgeräte ersetzt, die zuweilen selbst am Körper des Arbeitnehmers getragen werden: GPS-Geräte, Ausweise und Smartphone-Apps ermöglichen nunmehr die jederzeitige Ortung der Arbeitnehmer. Der Arbeitgeber kann deren Fortbewegungen folglich zeitlich und räumlich lokalisieren.

Diese Technologien ermöglichen dem für die Verarbeitung Verantwortlichen die Erfassung und Verarbeitung von personenbezogenen Daten wie der Arbeitszeit, der Identität des Fahrers, der Anzahl der eingelegten Pausen, der zurückgelegten Kilometerzahl oder gar der zurückgelegten Strecken. Diese neuen Systeme, die eine Vielzahl neuer Funktionen aufweisen, wie beispielsweise die Feststellung des Verlustes der aufrechten Position, stellen jedoch auch neue Gefahren für die Privatsphäre der Arbeitnehmer dar.

Angesichts des besonders stark in die Privatsphäre der Arbeitnehmer eingreifenden Charakters einer solchen Überwachung, unterliegt jedes Geolokalisierungsgerät einer Vorabgenehmigung seitens der CNPD und der Arbeitgeber muss eine bestimmte Anzahl an gesetzlichen und praktischen Erfordernissen erfüllen.

7.5.1. Welche Zielsetzungen kann der Arbeitgeber verfolgen?

Vor dem Einbau eines Geolokalisierungsgeräts muss der Arbeitgeber die Zielsetzungen festlegen, die er durch den Einsatz eines solchen Systems erreichen möchte.

In vielen Fällen kann es sich dabei um die nachstehenden Zwecke handeln:

- Optimierung des Arbeitsprozesses durch eine bessere Zuweisung der verfügbaren Mittel (z.B. Entsendung des dem Eingriffsort am nächsten gelegenen Fahrzeugs, Verwaltung der Fahrzeugflotte,...);
- Sicherstellung der Weiterverfolgung von Waren besonderer Beschaffenheit (gefährliche Güter, Lebensmittel);
- Weiterverfolgung und Nachweis der Ausführung einer Dienstleistung im Zusammenhang mit dem Einsatz eines Fahrzeuges (z.B. Eingriff in das Straßennetz, Müllabfuhr,...) zur Inrechnungstellung der Leistungen gegenüber den Kunden;
- Beitrag zur Sicherheit der Güter (Fahrzeuge, befördertes Material);
- Sicherstellung der Sicherheit der Arbeitnehmer;
- Vorbeugung und Feststellung des Eintritts von Angriffen auf die körperliche Unversehrtheit der betroffenen Personen;
- Überwachung der Arbeitszeiten der Arbeitnehmer (sofern dies nicht über andere Mittel erfolgen kann);
- Möglichkeit zur rechtzeitigen Alarmierung der Polizei oder des Rettungsdienstes im Falle einer Straftat oder eines Unfalls;
- usw.

Im Hinblick auf die seitens des Arbeitgebers geltend gemachten Zweckbestimmungen, überprüft die CNPD einerseits, ob diese Zweckbestimmungen durch mindestens einen der gesetzlich vorgesehenen Fälle gerechtfertigt sind, und andererseits, ob die Geolokalisierung im Verhältnis zu den seitens des Arbeitgebers beabsichtigten Zielsetzungen notwendig und verhältnismäßig ist.

7.5.2. In welchen Fällen ist die Geolokalisierung möglich?

Es obliegt der CNPD, zu überprüfen, ob die seitens des Arbeitgebers geltend gemachten Zweckbestimmungen mindestens einem der gesetzlich vorgesehenen Fälle entsprechen.

Die Überwachung der Arbeitnehmer am Arbeitsplatz ist nur möglich, wenn sie für die nachstehenden Zwecke notwendig ist:

7

7. Überwachungsarten

- für die Sicherheit und Gesundheit der Arbeitnehmer,
- zum Schutz der Unternehmensgüter,
- zur Kontrolle des Produktionsablaufs (ausschließlich auf Maschinenseite), oder
- im Rahmen der Arbeitsorganisation auf Basis von Gleitzeit nach Maßgabe des Arbeitsgesetzbuchs.

Sicherheit und Gesundheit der Arbeitnehmer

Der Rückgriff auf ein Geolokalisierungssystem kann als zulässig betrachtet werden, wenn er die Gewährleistung der Sicherheit der Arbeitnehmer ermöglicht. Dieses Zulässigkeitskriterium wird seitens der CNPD grundsätzlich akzeptiert, wenn die Tätigkeit der Arbeitnehmer des Antragstellers entweder aufgrund der Ausübung gefährlicher Arbeiten oder der Gefahr körperlicher Angriffe beispielsweise aufgrund des Wertes der sich in ihrer Verwahrung befindenden Güter (d.h. die sie an sich selbst oder in ihren Fahrzeugen befördern) eine Gefährdung ihrer körperlichen Unversehrtheit darstellen könnte.

Dieses Kriterium kann beispielsweise seitens eines Geldtransportunternehmens geltend gemacht werden. Angesichts der Bedeutung der von diesem verwahrten Gelder und Wertgegenständen ist es zulässig, dass der Arbeitgeber jedwedes während des Transports auftretende Problem aufdecken und insbesondere beim Auftreten von Problemen schnellstmöglich die Polizei alarmieren kann.

Schutz der Unternehmensgüter

In diesem Fall beabsichtigt der Arbeitgeber den Schutz seiner Unternehmensgüter, d.h. den Schutz der seinen Arbeitnehmern zur Verfügung gestellten Fahrzeuge, aber auch der von diesen beförderten Güter (Waren, Bargeld, Werkzeug,...). Im Falle eines Angriffs oder des Diebstahls des Fahrzeugs kann der für die Verarbeitung Verantwortliche das betreffende Fahrzeug und die entwendeten Güter nachverfolgen.

Die Polizeibehörden können folglich die genauen Fortbewegungen des Fahrzeugs orten und möglicherweise die Täter des Diebstahls fassen.

Kontrolle des Produktionsablaufs (ausschließlich auf Maschinenseite)

Aus den parlamentarischen Arbeiten zu dem Gesetz geht hervor, dass der Gesetzgeber unter dieser Zulässigkeitsbedingung zunächst lediglich den Fall der rein beiläufigen Überwachung der Arbeitnehmer im Zuge der hauptsächlichen Überwachung eines mechanischen Industrieproduktionssystems vom Typ Fertigungslinie in Erwägung gezogen hatte, um dessen ordnungsgemäßen Betrieb zu kontrollieren.

Die CNPD ist jedoch der Ansicht, dass diese Zulässigkeitsbedingung mittels eines Geolokalisierungssystems auf die Kontrollen der Leistungserbringung ausgedehnt werden kann. Diese Vorbedingung kommt dem seitens des Gesetzgebers ursprünglich in Erwägung gezogenen Fall nahe, da die Überwachung der Arbeitnehmer in beiden Fällen als nebensächlich zu betrachten ist. Die durch die Überwachung verfolgte Hauptzielsetzung besteht in beiden Fällen in der Kontrolle der seitens des Arbeitgebers im Rahmen seiner beruflichen Tätigkeit bereitgestellten materiellen Infrastruktur, der Maschinen und Werkzeuge. Die seitens des Arbeitgebers verfolgten Interessen sind demnach ähnlich, ungeachtet dessen, ob der Arbeitsprozess in der industriellen Herstellung oder in der Erbringung von Dienstleistungen besteht.

Im Rahmen der Arbeitsorganisation auf Basis von Gleitzeit erforderliche Datenverarbeitung

Bei der Arbeitsorganisation auf Basis von Gleitzeit handelt es sich um ein Organisationssystem, das den Arbeitnehmern die Möglichkeit einräumt, ihre Arbeitszeit und ihre Arbeitsdauer unter Einhaltung der vorab in Abhängigkeit von den Diensterfordernissen festgesetzten Zeitspannen nach persönlichem Belieben zu gestalten.

Die CNPD ist der Ansicht, dass ein Geolokalisierungssystem zur Verfolgung der Arbeitszeiten der Arbeitnehmer eingesetzt werden kann. Ausgehend von der Behauptung, dass die Gefährdung der Privatsphäre der Arbeitnehmer unabhängig von der seitens des Arbeitgebers gewählten Arbeitsorganisation (Gleitzeit oder feste Arbeitszeit) absolut identisch ist, gibt es für die CNPD kein Argument, das gegen den Rückgriff auf ein Geolokalisierungssystem im Rahmen einer Arbeitsorganisation auf Basis von Gleitzeit spricht. Vor jeder Genehmigung überprüft die CNPD jedoch, ob die Überwachung nicht durch andere Mittel erfolgen kann, die weniger stark in die Privatsphäre der Arbeitnehmer eingreifen. Darüber hinaus wird eine solche Überwachung nur dann genehmigt, wenn im Unternehmen tatsächlich ein Gleitzeitsystem mit vorgegebenen Zeitfenstern, usw. angewandt wird.

Überdies sei an dieser Stelle unterstrichen, dass ein Geolokalisierungssystem nicht gerechtfertigt ist, wenn der Arbeitnehmer seine Arbeit nach eigenem Belieben organisieren kann (z.B. im Falle eines Handelsvertreters).

7.5.3. Die an Bedingungen und Empfehlungen geknüpfte Vorabgenehmigung der CNPD

Wenn der für die Verarbeitung Verantwortliche ein Geolokalisierungsgerät einsetzen möchte, muss er bei der CNPD eine Vorabgenehmigung beantragen.

Neben dem Vorliegen einer oder mehrerer Zulässigkeitsgründe überprüft die CNPD, ob der Rückgriff auf die Geolokalisierung im Verhältnis zu den seitens des Arbeitgebers geltend gemachten Zweckbestimmungen notwendig und verhältnismäßig ist.

Die Geolokalisierungssysteme werfen die heikle Frage auf, welches Maß an Kontrolle auf einem Arbeitnehmer während seiner gesamten Arbeitszeit lasten darf, d.h. die Frage nach der Grenze zwischen Arbeit und Privatsphäre.

Der Grundsatz der Verhältnismäßigkeit beinhaltet, dass der für die Verarbeitung Verantwortliche die Verarbeitung auf Daten beschränken muss, die in Anbetracht der zu erzielenden Zweckbestimmungen angemessen und zutreffend sind und nicht darüber hinausgehen[46] und die Verarbeitungen nicht unverhältnismäßig sein dürfen.

Wie wir bereits vorher gesehen haben, stellen diese neuen Systeme deutlich neue Gefahren für die Privatsphäre der Arbeitnehmer dar. Die Rechte des Arbeitgebers sind mit den Rechten und Freiheiten der Arbeitnehmer in Einklang zu bringen. Die gesetzlichen Bestimmungen im Datenschutzbereich dürfen demnach nicht von den Bestimmungen des Arbeitsrechts getrennt werden. Daraus ergibt sich, dass die Überwachung einen möglichst geringen Eingriff in die Privatsphäre darstellen muss und der Arbeitnehmer sich das Recht auf eine anonyme Fortbewegung bewahren muss.

Der Gesetzgeber hat klare Einschränkungen vorgesehen, um das Eindringen der Geolokalisierungsgeräte in die Privatsphäre zu verringern. Diese sind insbesondere in den Genehmigungen der CNPD präzisiert und entstammen den allgemeinen Grundsätzen des Datenschutzgesetzes.

7.5.3.1. Verbot einer ständigen Überwachung

Ein Geolokalisierungssystem kann nicht mit der Zielsetzung einer ständigen Kontrolle der Arbeitnehmer eingesetzt werden, da es ansonsten als elektronische „Beschattung" betrachtet wird, die zwangsläufig den Schutz der Privatsphäre der betroffenen Personen gefährdet. Außer in präzisen und sehr beschränkten Ausnahmefällen sieht das Gesetz lediglich die zeitweilige und überdies unter bestimmten restriktiven Bedingungen erfolgende Überwachung des Arbeitnehmers vor.

46 Artikel 4, Absatz (1), Buchstabe (b) des abgeänderten Gesetzes vom 2. August 2002.

7

7. Überwachungsarten

7.5.3.2. Verbot der Überwachung aller Leistungen der Arbeitnehmer

Die seitens des Arbeitgebers zusammengetragenen Daten dürfen nicht zur Überwachung der Leistungen und/oder des Verhaltens der Arbeitnehmer dienen, die außerhalb der Zweckbestimmungen liegen, auf die die Genehmigung der CNPD gründet.

So darf der für die Verarbeitung Verantwortliche nicht aus den Augen verlieren, dass die durch die Überwachung beabsichtigte Hauptzielsetzung in der Kontrolle seiner materiellen Infrastruktur, einschließlich seiner Fahrzeuge und der darin eingelagerten Güter besteht und die Überwachung der Arbeitnehmer demnach nur nebensächlich erfolgt.

7.5.3.3. Verbot der Kontrolle der Arbeitnehmer außerhalb der Arbeitszeiten

Sofern der Arbeitnehmer dazu befugt ist, den Dienstwagen zu Privatzwecken, d.h. außerhalb der Arbeitszeiten zu nutzen, muss ihm der Arbeitgeber zwangsläufig die Möglichkeit zur Deaktivierung des Geolokalisierungsgeräts einräumen. In keinem Fall hat der Arbeitgeber das Recht, den Arbeitnehmer außerhalb seiner Arbeitszeiten zu überwachen. An dieser Stelle sei jedoch anzumerken, dass das Geolokalisierungssystems im Falle einer ausschließlich dienstlichen Nutzung des Fahrzeugs ständig aktiviert sein kann.

7.5.3.4. Verbot der Kontrolle der Einhaltung der Geschwindigkeitsbegrenzungen

Der Arbeitgeber kann keine Daten in Bezug auf Geschwindigkeitsüberschreitungen verarbeiten. Dieses Verbot wird ausdrücklich in Artikel 8, Absatz (2) des abgeänderten Gesetzes vom 2. August 2002 genannt, der festsetzt, dass *„die Verarbeitung von Daten bezüglich strafbarer Handlungen (...) nur in Ausführung einer Gesetzesbestimmung erfolgen kann"*. Die nachstehenden Daten stellen kein Problem dar: Geolokalisierungsdaten (Positionsbestimmung und Strecken-verlauf), ergänzende Daten wie Nutzungsdatum und Nutzungsdauer des Fahrzeugs, Fahrzeit, zurückgelegte Kilometerzahl, Uhrzeit des Tätigkeitsbeginns und des Tätigkeitsendes, usw.

7.5.3.5. Begrenzte Speicherdauer

Die Lokalisierungsdaten dürfen nur über einen Zeitraum von maximal zwei Monaten gespeichert werden.

Im Falle eines Zwischenfalls können die Daten im Rahmen ihrer Weitergabe an die zuständigen Justizbehörden zur Feststellung oder Verfolgung von Straftaten jedoch länger als oben genannt gespeichert werden.

Die rein technischen Daten und Parameter in Bezug auf das Fahrzeug können länger als zwei Monate gespeichert werden, jedoch vorausgesetzt, dass die personenbezogenen Daten der Verarbeitung zuvor gelöscht oder anonymisiert wurden.

Abschließend können die Daten in Bezug auf die Arbeitszeiten über einen Zeitraum von maximal drei Jahren gespeichert werden, was der in Artikel 2277, Absatz 1 des Zivilgesetzbuchs festgesetzten Verjährungsfrist für Gehaltsklagen der Arbeitnehmer entspricht.

7.6. Zutrittsüberwachung und Kontrolle der Arbeitszeiten

Die Überwachung des Zutritts zu den Räumlichkeiten und die Kontrolle der Arbeitszeiten mittels Firmenausweis/Karte oder Code, die eine direkte oder indirekte Identifizierung des jeweiligen Arbeitnehmers ermöglichen, fallen unter die Verarbeitung personenbezogener Daten und unterliegen folglich den Vorschriften des Datenschutzgesetzes.

Die Zutrittsüberwachungssysteme dienen der Verwaltung und Kontrolle der physischen Zugänge an den Eingängen von Standorten, Gebäuden, Räumlichkeiten sowie zu bestimmten einschränkend festgelegten zutrittsbeschränkten Bereichen.

Die im Rahmen der Arbeitsorganisation auf Basis von Gleitzeit oder auf Basis fester Arbeitszeiten eingesetzten Systeme zur Kontrolle der Arbeitszeiten dienen der Verwaltung und Kontrolle der Arbeits- und Anwesenheitszeiten am Arbeitsplatz.

Um dem Arbeitgeber den Verwaltungsaufwand zu erleichtern, hat die CNPD für diese Verarbeitungen darüber hinaus eine Sammelgenehmigung eingerichtet.

7.6.1. Welche Zielsetzungen kann der Arbeitgeber verfolgen?

Kontrolle des Zutritts zu den Räumlichkeiten

Die Verarbeitung personenbezogener Daten in Bezug auf die **Arbeitnehmer** darf nur zu den nachstehenden Zwecken erfolgen:

- für die Sicherheit und Gesundheit der Arbeitnehmer, vorbehaltlich der vorherigen Einholung der Zustimmung des gegebenenfalls eingerichteten gemischten Betriebsrats,
- für den Schutz der Unternehmensgüter (in diesem Fall ist die Zustimmung des gemischten Betriebsrats nicht erforderlich).

Die Verarbeitung von Daten **Dritter** darf nur unter den nachstehenden Voraussetzungen erfolgen:

- sofern die betroffene Person ihre Einwilligung erteilt hat (im Sinne der Definition aus Artikel 2, Buchstabe (c) des Gesetzes vom 2. August 2002), oder
- in der unmittelbaren Umgebung oder an jedem anderen öffentlich zugänglichen oder nicht zugänglichen Ort außer in Wohnräumen, insbesondere in Parkhäusern, Bahnhöfen, Flughäfen und in den öffentlichen Transportmitteln, vorausgesetzt, dass der jeweilige Ort durch seine Art, seine Lage, seine Beschaffenheit oder seine Nutzung ein Risiko darstellt, das die Datenverarbeitung für die Sicherheit der Benutzer oder für die Verhütung von Unfällen erforderlich macht, oder
- an den privaten Zutrittsorten, an denen die dort niedergelassene natürliche oder juristische Person der für die Verarbeitung Verantwortliche ist.

Kontrolle der Arbeitszeiten

Die Verarbeitung personenbezogener Daten in Bezug auf die **Arbeitnehmer** ist nur erlaubt, wenn dies im Rahmen einer Arbeitsorganisation auf Basis von Gleitzeit in Übereinstimmung mit dem Gesetz erforderlich ist, vorbehaltlich der vorherigen Einholung der Zustimmung des gegebenenfalls eingesetzten gemischten Betriebsrats.

Dies betrifft folglich alle Datenverarbeitungen, die zum Zweck der Kontrolle der Anwesenheitszeiten der

7

7. Überwachungsarten

Arbeitnehmer, der Identifikation der Arbeitnehmer an Ein- und Ausgängen, der obligatorischen Kernzeiten sowie der Prüfung der Beachtung der Ausgleichsregelungen und deren Auswirkung auf den Lohn und den Urlaubsausgleich durchgeführt werden.

Demnach stellt sich die Frage, ob der Arbeitgeber auch die festen Anwesenheitszeiten überwachen kann, da in Artikel L.261-1, Absatz (1), Punkt (5) ausdrücklich und ausschließlich auf eine Arbeitsorganisation „auf Basis von Gleitzeit nach Maßgabe des vorliegenden Gesetzbuchs verwiesen wird".

Diesbezüglich ist die Nationale Kommission der Ansicht, dass eine Unterscheidung zwischen einer Arbeitsorganisation auf Basis von Gleitzeit und einer Arbeitsorganisation auf Basis fester Arbeitsstunden jedweder Grundlage entbehre und der Organisation und dem ordnungsgemäßen Betrieb des Unternehmens abträglich sei. Darüber hinaus würde diese Unterscheidung bedeuten, dem Arbeitgeber die mittels jedweden technischen Mittels erfolgende Messung der Anwesenheitszeiten der Arbeitgeber zu verbieten, die auf Basis einer festen Arbeitszeit arbeiten, und daraus gegebenenfalls den genauen Betrag der ihnen nach Maßgabe der tatsächlich geleisteten Stunden zustehenden Bezahlung abzuleiten.

Ausgehend von der Behauptung, dass die Privatsphäre der Arbeitnehmer unabhängig von der seitens des Arbeitgebers gewählten Arbeitsorganisation (Gleitzeit oder feste Arbeitszeiten) stets gleich stark gefährdet ist und dass diese Art der Überwachung aus Sicht des Gesetzgebers nicht als übertrieben betrachtet wird, ist die Nationale Kommission in diesem Fall der Ansicht, dass eine solche Überwachung ungeachtet der restriktiven Formulierung des Zulässigkeitskriteriums in Artikel L.261-1, Absatz (1), Punkt (5) seitens des Arbeitgebers durchgeführt werden darf.

Was die Kontrolle der Arbeitszeiten **Dritter** betrifft, so sei darauf hingewiesen, dass die Maßnahmen zur Überwachung der Arbeitszeiten und der Anwesenheitszeiten am Arbeitsplatz grundsätzlich nur die Arbeitnehmer des für die Verarbeitung Verantwortlichen betreffen. Es gibt jedoch Fälle, in denen Dritte (z.B. die Beschäftigten eines Unterauftragnehmers, Lieferanten, usw.) über einen mehr oder weniger langen Zeitraum hinweg in den Räumlichkeiten des für die Verarbeitung Verantwortlichen Leistungen erbringen und demnach einer solchen Überwachung unterliegen, was insbesondere der Überprüfung der Übereinstimmung mit den seitens des für die Verarbeitung Verantwortlichen unterzeichneten Dienstleistungsverträgen dient. In diesen Fällen hält die CNPD fest, dass die einzige Zulässigkeitsbedingung, die in diesem Fall Anwendung finden könnte, die ausdrückliche und unmissverständliche Einwilligung des externen Arbeitnehmers ist.

7.6.2. Die an Bedingungen geknüpfte Vorabgenehmigung der CNPD

Jedes Mal, wenn ein Arbeitnehmer einen Firmenausweis, eine Magnetkarte oder einen Code verwendet, zeichnet das System ihn betreffende Daten auf. Diese Aufzeichnungen können verwendet werden, um die Fortbewegungen „nachzuverfolgen" und bergen Gefahren der Zweckentfremdung.

Um diese Gefahren auf ein Mindestmaß zu begrenzen, verpflichtet sich der Arbeitgeber zur Einhaltung der in den Genehmigungen der CNPD genannten Bedingungen.

Zweckbestimmung der Verarbeitung

Die eingesetzte Verarbeitung in Bezug auf die **Zugangsüberwachung** darf ausschließlich der Kontrolle der Ein- und Ausgänge der Standorte, Gebäude und Räumlichkeiten des Arbeitgebers dienen. Sie darf nicht zweckentfremdet werden, d.h. nicht zur Kontrolle der Fortbewegungen im Inneren des Arbeitsortes verwendet werden, außer in Fällen, in denen bestimmte festgelegte Bereiche Gegenstand einer mit der Sicherheit der Güter und der dort tätigen Personen begründeten Zutrittsbeschränkung sind.

Was die **Überwachung der Arbeitszeiten** betrifft, so dürfen die seitens des Arbeitgebers erfassten Daten ausschließlich zur Verwaltung und Überprüfung der Ankunftszeiten am Arbeitsplatz und der Zeiten des Verlassens des Arbeitsplatzes verwendet werden.

Speicherdauer

Eine begrenzte Speicherdauer der Daten stellt eine zusätzliche Garantie zur Vermeidung möglicher Zweckentfremdungen dar.

Was die Zugangsüberwachung betrifft, so dürfen die Daten nicht länger als drei Monate ab ihrer Aufzeichnung gespeichert werden, es sei denn, die Verarbeitung bezieht sich gleichzeitig auch auf die Kontrolle der Arbeitszeiten (wenn beispielsweise ein einziger Firmenausweis für beide Zwecke verwendet wird). In diesem Fall dürfen die personenbezogenen Daten der Arbeitnehmer und der diesen gleichgestellten Personen nicht länger als drei Jahre gespeichert werden[47].

Personenbezogene Daten von Angestellten des öffentlichen Dienstes dürfen nicht länger als fünf Jahre gespeichert werden[48].

Im Falle einer Anfechtung oder eines Zwischenfalls müssen die sich darauf beziehenden Daten nicht nach Ablauf der oben genannten Fristen vernichtet werden, sofern sie an die zuständigen Behörden weitergeleitet werden.

7.6.3. Vereinfachte Formalitäten

Die vorstehend analysierten beiden Verarbeitungsarten unterstehen der Regelung der Vorabgenehmigung seitens der CNPD. Da sich die CNPD darüber bewusst ist, dass eine große Anzahl von Arbeitgebern diese Maßnahmen einsetzt und die seitens der für die Verarbeitung Verantwortlichen vorab zu erfüllenden Verwaltungsformalitäten vereinfachen wollte, hat sie ein vereinfachtes Genehmigungsverfahren eingesetzt (Sammelgenehmigung[49]). Dies gilt jedoch nicht für die biometrischen Systeme, die weiterhin dem üblichen Genehmigungsverfahren unterliegen[50].

Durch **Sammelgenehmigung** kann die CNPD allgemein bestimmte Datenverarbeitungen genehmigen, die:

- ein und dieselbe Zweckbestimmung verfolgen,
- sich auf identische Datenkategorien beziehen und
- ein und dieselben Empfänger bzw. Empfängerkategorien haben.

Zum Erhalt einer Sammelgenehmigung übermittelt der für die Verarbeitung Verantwortliche an die CNPD eine **formelle Verpflichtung**, durch die er erklärt, dass die Verarbeitung mit der in der Sammelgenehmigung enthaltenen Beschreibung übereinstimmt.

47 *Diese Frist entspricht den Bestimmungen aus Artikel 2277 des Zivilgesetzbuchs.*

48 *Siehe **Verwaltungsgericht, 11. Juni 1998, Nr. 10607C**.*

49 *Beschluss Nr. 63/2007 vom 22. Juni 2007: Sammelbeschluss in Bezug auf die Verarbeitung personenbezogener Daten zwecks Überwachung der Arbeitszeiten im Rahmen einer Arbeitsorganisation gemäß Gleitzeit Beschluss Nr. 64/2007 vom 22. Juni 2007: Sammelbeschluss in Bezug auf die Verarbeitung personenbezogener Daten zwecks Zutrittsüberwachung*

50 *Siehe Punkt 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