CHAPITRE 3
L'UTILISATION DE CAMÉRAS ET LA LOI SUR LA VIE PRIVÉE

Dominique Pissoort
Paul De Hert

Les caméras sont utilisées de plus en plus pour des applications qui se multiplient. Ainsi, on les retrouve sur les lieux de travail, que ce soit pour assurer la sécurité des locaux ou pour surveiller la productivité des travailleurs, elles sont également utilisées à des fins privées dans des halls d'entrée d'immeubles à appartement. On les retrouve également auprès de diverses professions telles que la presse (but d'information), la police (but de surveillance et constatation d'infraction), les détectives privés...

Le présent chapitre est subdivisé en trois sections : l'utilisation des caméras de surveillance de façon générale, le droit à l'image et l'utilisation de caméras par la presse et enfin l'utilisation de caméras par la police.

3.1. SECTION 1 : L'UTILISATION DES CAMÉRAS DE SURVEILLANCE

3.1.1. Application de la LVP aux caméras

3.1.1.1. La directive européenne du 24 octobre 1995

D'après le préambule de la directive européenne du 24 octobre 1995, la directive est explicitement applicable à la matière de la surveillance par caméras. Cette directive impose à notre pays d'adapter sa législation interne aux nouvelles normes européennes, y compris sur le plan de la surveillance par caméras. Les considérants 14, 15 et 16 du préambule de la directive disent ce qui suit: *« Considérant que, compte tenu de l'importance du développement en cours, dans le cadre de la société de l'information, des techniques pour capter, transmettre, manipuler, enregistrer, conserver ou communiquer les données constituées par des sons et des images, relati-*

ves aux personnes physiques, la présente directive est appelée à s'appliquer aux traitements portant sur ces données;

Considérant que les traitements portant sur de telles données ne sont couverts par la présente directive que s'ils sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause;

Considérant que les traitements des données constituées par des sons et des images, tels que ceux de vidéosurveillance, ne relèvent pas du champ d'application de la présente directive s'ils sont mis en œuvre à des fins de sécurité publique, de défense, de sûreté de l'État ou pour l'exercice des activités de l'État relatives à des domaines du droit pénal ou pour l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit communautaire ».

3.1.1.1.1. Trois remarques sur le passage relatif aux caméras de la directive européenne

Hormis ces considérants, le texte de la directive ne revient pas sur les traitements visuels. On peut faire trois remarques à cet égard. *Tout d'abord*, la directive est très vague sur la manière dont les Etats membres doivent intégrer et appliquer le contenu de la directive à la matière des traitements visuels. La question de savoir par exemple si la directive s'applique aux systèmes de surveillance par caméras sans enregistrement d'images fait l'objet de désaccords. Bien qu'il faille admettre que, sur la base de la très large définition de la notion de 'traitement' de l'article 2 de la directive, c'est le cas[1], on pense par exemple chez nous et dans d'autres pays voisins que les systèmes de surveillance par caméras sans enregistrement d'images n'entrent pas dans le champ d'application de la directive[2]. Bien que cette question puisse à l'avenir faire l'objet d'un avis du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, qui est compétent en vertu

1. La directive donne la définition suivante: *« Toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».*
2. Comp. BOULANGER, M.H., DE TERWANGNE, C., LEONARD, T., LOUVEAUX, S., MOREAU, D. et POULLET, Y., « La protection des données à caractère personnel en droit communautaire », *J.T.D.E.*, 1997, 122-123.

de l'article 30 de la directive pour se prononcer sur l'application de la directive, ou d'une question adressée à la Cour de justice de Luxembourg, il est souhaitable de ne pas attendre pour élaborer une réglementation de la matière qui donne forme à l'application de la directive sur la problématique.

En deuxième lieu, les considérants cités nous apprennent que la directive n'est applicable que si les traitements sur les données visuelles sont automatisés ou si les données sur lesquelles ils portent sont contenues ou sont destinées à être contenues dans un fichier structuré selon des critères spécifiques relatifs aux personnes, afin de permettre un accès aisé aux données à caractère personnel en cause. Il ressort cependant de notre analyse qu'il est nécessaire que nous ayons une initiative plus ambitieuse dans notre pays, et que les données visuelles à caractère personnel qui ne satisfont pas à ces conditions soient également visées. Pensons simplement à la photo prise en secret d'une personne qui se trouve dans un lieu non accessible au public, photo qui n'est pas reprise ensuite dans un fichier. Ce raisonnement vaut ipso facto pour le simple fait d'épier une personne.

Une telle initiative devrait également être par exemple applicable à la surveillance par caméras, où des personnes sont filmées mais où les données obtenues ne peuvent être considérées comme des données à caractère personnel au sens de la directive[1]. Pensons à l'utilisation de matériel d'observation thermique qui permet par exemple d'avoir une image du corps de personnes se trouvant dans une habitation fermée. On peut également penser aux caméras qui observent la circulation – qui ne sont pas réglementées par la loi du 4 août 1996 (infra) – et qui dans la situation belge actuelle ne peuvent réaliser d'images de marques d'immatriculation ou des passagers des véhicules – et qui ne fournissent donc pas de données à caractère personnel au sens de la directive – mais qui sont susceptible de le faire à l'avenir en s'appuyant sur une technologie plus puissante. Il est souhaitable de ne pas attendre ce moment et de créer dès maintenant un cadre pour ces caméras de la circulation.

En troisième lieu, la directive n'est pas applicable aux traitements de données constituées par des images s'ils sont mis en œuvre par exemple à des fins de sécurité publique, pour l'exercice des activités de l'Etat relatives au droit pénal et en vue de l'exercice d'autres activités qui ne relèvent pas du champ d'application du droit

1. Cf. article 2 de la directive: *« Aux fins de la présente directive, on entend par: a) 'données à caractère personnel' : toute information concernant une personne physique identifiée ou identifiable (personne concernée); est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale; ».*

communautaire (cf. le troisième considérant de la circulaire cité plus haut). Il faut également élaborer une réglementation pour ces finalités.

Ces remarques valent ipso facto pour la loi belge sur la vie privée telle que modifiée par la loi transposant la Directive 95/46/CE du 24 octobre 1995 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[1]. Cette modification peut en effet en grande partie être considérée comme une transposition fidèle de la directive européenne, ce qui fait que les trois remarques valent identiquement pour le droit belge. Il y a cependant lieu de souligner que le contenu de la directive est également rendu applicable en Belgique aux traitements par la police, les services de sécurité et autres instances exclues dans la directive.
Certains problèmes évoqués pour l'application dans leur chef de techniques d'espionnage et de prises de vues ainsi que de surveillance par caméras dans le sens du présent projet peuvent par conséquent être résolus sur la base de la loi sur la vie privée modifiée, mais pas tous (supra).

3.1.1.2. Le point de vue de la Commission

La Commission de la protection de la vie privée a, à plusieurs reprises, sur la base de ses compétences, contribué activement à la mise en place de 'directives' relatives à la matière des caméras et de la surveillance visuelle. Ainsi, la Commission, dans son avis n° 14/95 du 7 juin 1995, avait souligné que la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel est applicable au traitement d'images à condition que la vidéo filme des 'données à caractère personnel' et que les données soient enregistrées sur bande. Dans un nouvel avis du 13 décembre 1999 (n° 34/1999), la Commission souligne la nécessité d'adapter les principes développés dans son avis n° 14/95, à la lumière de l'approbation de la loi du 11 décembre 1998, qui a modifié certains points essentiels de la loi du 8 décembre 1992[2].

La principale nouveauté est l'élargissement du champ d'application de la LVP.

---

1. Loi du 11 décembre 1998 transposant la directive 95/46/EG du 24 octobre 1995 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, *M.B.,* 3 février 1999. Cette loi n'est pas encore entrée en vigueur.
2. Commission de la protection de la vie privée, avis n° 34/1999 du 13 décembre 1999 relatif aux traitements d'images effectués en particulier par le biais de systèmes de vidéosurveillance.

La loi du 11 décembre 1998 étend son application à « toute opération ». Cela signifie qu'une opération automatisée individuelle, et donc unique, entre également dans le champ d'application de la loi. Cet élément est particulièrement important en ce qui concerne la mise en œuvre unique ou de courte durée d'un système de surveillance par caméra. Il n'est pas non plus nécessaire que les données soient conservées pour que l'on ait un traitement, dès lors que le traitement est automatisé. En effet, la collecte constitue en elle-même un traitement. La conservation des données enregistrées n'est donc plus une condition nécessaire à l'application de la loi: elle s'applique dès le moment où les images sont filmées.

En application de l'article 9 de la LVP, le propriétaire du système vidéo est obligé d'annoncer ce système d'une façon ou d'une autre. L'apposition, à proximité de l'appareil, d'un avis lisible qui contient les éléments d'information requis satisfait à cette obligation. En ce qui concerne l'utilisation de systèmes de vidéosurveillance pour la protection de personnes et de biens, la Commission souligne que la collecte de données dans des lieux publics et accessibles au public doit être considérée comme proportionnelle si elle a lieu dans le cadre de la prévention et de la constatation d'infractions dans des lieux particulièrement dangereux (par exemple dans le cadre des transports de fonds). L'évaluation doit être plus stricte si les systèmes de vidéosurveillance sont utilisés dans des lieux non accessibles au public. Dans ce cas, l'évaluation est plus stricte et la Commission examine notamment si le propriétaire du système a obtenu l'autorisation des personnes concernées. Dans tous les cas, le traitement d'images doit constituer un *moyen adéquat et nécessaire* pour atteindre l'objectif fixé et doit rester un moyen *subsidiaire* d'atteindre cet objectif. Dans ce qui suit, nous nous arrêterons à quelques passages de l'avis.

3.1.1.2.1. Le champ d'application

Comme on vient de l'exposer, la loi du 11 décembre 1998 étend son application à « tout traitement ». Cela signifie qu'un traitement automatisé individuel, et donc unique, entre également dans le champ d'application de la loi. Cet élément est particulièrement important en ce qui concerne la mise en service unique ou de courte durée d'un système de surveillance par caméra.

La notion de « traitement d'images » s'étend donc désormais à tout système de prise de vues, analogique ou numérique, continue ou discontinue, avec ou sans conservation de ces prises de vues, sur quelque support que ce soit. Cette notion s'applique en particulier à l'utilisation de caméras. On admet que la notion est également applicable aux appareils photo.

3.1.1.2.2. Une typologie des applications

L'avis 34/99 de la Commission débute par une typologie des domaines d'application des traitements d'images. La Commission distingue à cet égard ce qui suit en ce qui concerne les possibilités d'utilisation et/ou les objectifs de l'utilisation de caméras

– *Usage privé:*

Le traitement d'images à usage privé est destiné à la constitution d'archives temporaires ou permanentes pour l'individu, le cercle familial ou les proches, à des fins d'usage domestique ou personnel[1].

– *Traitement par les médias:*

Usage informatif (journalisme)

Ce type de traitement est celui réalisé par exemple par des professionnels de l'information, à des fins de journalisme, et dont le résultat est destiné à être diffusé principalement auprès de personnes n'ayant pas participé à l'événement saisi, tel que: reportage de la presse écrite ou télévisée, ...

Usage artistique

On vise ici le traitement réalisé, par exemple, par des professionnels du cinéma ou de la télévision, et dont le résultat, photos ou films, est destiné à être diffusé principalement auprès de personnes n'ayant pas participé à l'événement saisi, tel que : film, téléfilm, diffusion (d'extraits) d'une représentation théâtrale, d'un concert, ...

Usage récréatif

Il concerne le traitement d'images réalisé en particulier par des professionnels du cinéma ou de la télévision, et dont le résultat est destiné à être diffusé principalement auprès de personnes n'ayant pas participé à l'événement saisi, tel que: émission TV, caméra cachée, talk-show, ...

1. Conformément à l'article 3, § 2 de la Loi du 8 décembre 1992 tel que modifié par la Loi du 11 décembre 1998, ci-après dénommée « la loi ».

– *Vidéosurveillance:*

Plusieurs finalités peuvent être regroupées sous la notion de vidéosurveillance: la protection des biens et des personnes, en ce compris le contrôle d'accès à certains bâtiments, le contrôle du trafic routier et la prévention des infractions connexes, le contrôle de l'activité sur les lieux de travail. Le contrôle des habitudes du consommateur, à des fins de marketing, est une quatrième finalité fort importante.

a) Concernant la protection des biens et des personnes:

Les mesures prises en vue de la protection des biens et personnes se traduisent de plus en plus souvent par une surveillance par caméra, avec ou sans conservation des images captées. Trois types de lieux où s'opère ce type de surveillance peuvent à cet égard être distingués: 1) lieux fermés non accessibles au public[1]; 2) lieux fermés accessibles au public[2]; 3) lieux ouverts[3].

b) Concernant le contrôle de la circulation:

La Commission distingue les dispositifs à vocation non identifiante, qui contrôlent par exemple la fluidité du trafic (réglage de la cadence des feux de circulation, détournement de trafic, ...), des dispositifs à vocation identifiante tels que ceux destinés à la constatation d'infractions au Code de la route (radars).

c) Concernant la recherche observationnelle:

Les traitements visés sont ceux réalisés par (ou pour) des professionnels du marketing, dont la finalité est l'observation du comportement du consommateur à l'intérieur d'un magasin et dont le résultat est destiné à l'organisation des points de vente.

---

1. L'on vise les bâtiments ou enceintes fermés destinés uniquement à l'usage de leurs occupants habituels (habitation familiale, immeubles à appartements, bâtiments à usage de bureaux, usines, fermes,... à l'exclusion de l'espace d'accès principal au lieu considéré).
2. Sont visés les bâtiments ou enceintes fermés destinés à l'usage du public, notamment en vue de l'exercice d'un service envers ce public (commerces, salles de guichets de banques, d'assurances, cinémas, restaurants, hôtels, mais également transports en commun, accès principal d'un immeuble, d'une propriété, salles de spectacles, salles et terrains de sport ou de jeux, locaux administratifs, ...).
3. Ce sont les espaces non délimités par une enceinte, et accessibles librement au public (voie publique, parcs, ...).

d) Concernant le contrôle de l'activité sur les lieux de travail:

Les traitements visés sont ceux réalisés par un employeur et destinés au contrôle de l'activité professionnelle des employés.

La description qui précède vise à schématiser les utilisations les plus fréquentes des techniques de traitement d'images. Elle ne constitue cependant pas une liste de définitions juridiques et ne prétend pas être exhaustive.

La Commission souligne à bon droit que ces traitements, quelle que soit leur spécificité, restent soumis – à l'exception des traitements à des fins personnelles ou domestiques – aux différents principes fondamentaux de la loi du 8 décembre 1992 développés ci-dessous.

3.1.1.2.3. Obligations d'information

Conformément à l'article 9 de la LVP, la personne physique auprès de laquelle des données à caractère personnel sont recueillies afin d'être traitées doit être informée d'un certain nombre d'éléments. Cet article ne stipule pas la manière dont cette information doit se dérouler. La Commission a considéré dans son avis n° 14/95 qu'une information collective consistant en la suspension, aux alentours de l'appareil d'enregistrement[1], d'un avis lisible comportant les éléments d'information nécessaires, satisfait à cette obligation. Cette directive est maintenue.

L'obligation d'information concerne, quant au contenu, le nom et l'adresse du responsable du traitement ou de son représentant, les finalités du traitement, l'existence d'un droit d'accès et de rectification des personnes concernées[2], les destinataires ou les catégories de destinataires des données.

L'information relative à la finalité visée doit être indiquée de façon appropriée et suffisamment claire et détaillée afin que toutes les personnes concernées soient conscientes du fait qu'elles sont visées par la mesure. Un avis trop général mentionnant la protection d'un magasin contre le vol pourrait ainsi laisser penser aux employés que seule est visée la prévention du vol dans les rayons par les clients,

1. Par exemple dans le cas d'une caméra située dans un lieu fermé accessible au public, aux endroits d'accès à ce lieu; dans le cas d'un lieu ouvert, à proximité immédiate de la caméra.
2. Certains aménagements à ce droit propres au contexte du traitement d'images sont développés ci-après.

alors que la mesure viserait également – et la caméra serait également dirigée vers – la surveillance des employés responsables de l'encaissement des achats.

Une dérogation à cette obligation d'information ne peut être admise que dans le cadre de l'article 3, §§ 3, 4, 5 et 6 de la LVP. Les exceptions concernent en particulier le traitement de données à caractère personnel à des fins de journalisme ou d'expression artistique ou littéraire, ainsi que les traitements gérés par les services de renseignement et de police.

3.1.1.2.4. Choix de finalités clairement définies et légitimes

En vertu de l'article 4 de la loi, le traitement doit se dérouler pour des finalités clairement définies et légitimes. La détermination de la finalité du traitement est un élément essentiel de la protection des personnes. Elle aura des conséquences directes sur les modalités d'application de la loi. Elle permettra en outre d'identifier les traitements qui ne tombent pas dans le champ d'application de la loi[1].
Un traitement à des fins de journalisme, d'expression artistique ou littéraire se trouvera exempté de certaines obligations prévues par la loi (voyez *supra* et article 3, § 3).

Dès lors que la détermination de la finalité du traitement entraîne l'application de la loi, le responsable du traitement devra s'assurer du respect des différentes conditions de l'article 4 et en particulier du *caractère légitime de la finalité*[2]. Il est par conséquent essentiel que la finalité soit déterminée de façon suffisamment précise par le responsable du traitement.

La Commission rappelle que la légitimité des traitements d'images doit être jugée en application du *principe de proportionnalité* visé à l'article 4 de la LVP: l'intérêt

1. Cf. article 3, § 2: traitement d'images effectué à des finalités exclusivement personnelles ou domestiques.
2. Ce caractère légitime peut découler de différentes hypothèses mentionnées à l'article 5 de la loi: lorsque la personne concernée a indubitablement donné son consentement (article 5, a.); lorsque le traitement est nécessaire à l'exécution d'un contrat (article 5, b.); lorsqu'il est nécessaire à l'exécution d'une loi, d'un décret ou d'une ordonnance (article 5, c.) (rentreraient dans cette hypothèse certains traitements effectués par exemple dans le cadre de l'arrêté royal du 12 septembre 1999 concernant l'installation et le fonctionnement de caméras de surveillance dans les stades de football); lorsqu'il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée (article 5, d.); lorsqu'il est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique (article 5, e.); et dans le respect de la balance des intérêts du responsable du traitement et de la personne dont les données sont collectées (article 5, f.).

général ou les intérêts légitimes du gestionnaire du traitement doivent être mis en balance avec le droit à la protection de la vie privée de la personne enregistrée.
En ce qui concerne par exemple l'utilisation de caméras de vidéosurveillance pour la protection des personnes et des biens, la collecte de données dans les lieux publics et accessibles au public peut être considérée comme proportionnelle lorsqu'elle se déroule dans le cadre de la prévention et de la constatation d'infractions dans des endroits particulièrement dangereux (par exemple dans le cadre de transferts de fonds). L'appréciation pourrait être plus stricte lorsque les caméras de vidéosurveillance sont utilisées dans des lieux non accessibles au public. L'exigence du consentement des personnes concernées pourrait ici entrer en ligne de compte dans l'appréciation du respect du critère de proportionnalité.
Entre également dans l'appréciation du respect de ce critère la conservation ou l'absence de conservation des données par le responsable du traitement.

Il convient en tout état de cause de garder à l'esprit qu'un traitement d'images doit être un *moyen adéquat et nécessaire* à la réalisation de l'objectif poursuivi[1].
Il doit en outre rester un moyen *subsidiaire* de parvenir à cet objectif. Une installation de caméras de vidéosurveillance devra s'avérer indispensable pour atteindre l'objectif poursuivi, d'autres mesures moins attentatoires à la vie privée s'avérant insuffisantes dans le cas d'espèce. En ce sens, la sécurité d'un local pourra dans certains cas être aussi bien protégée par des mesures peu intrusives, telles qu'un verrouillage renforcé des portes et un système d'alarme, que par un système de vidéosurveillance.

3.1.1.2.5. Respecter le but initial de la caméra

Le principe de finalité implique également que les images traitées *ne peuvent être utilisées d'une manière incompatible* avec le but clairement défini et légitime. En d'autres termes, les données ne peuvent être utilisées que dans le cadre de la finalité déclarée et ne peuvent donner lieu à d'autres utilisations.

1. Dans le contexte actuel de multiplication des systèmes de vidéosurveillance à des fins de sécurité, il convient de remarquer que l'utilisation de tels systèmes ne constitue pas le remède absolu contre la criminalité. De la même façon qu'une voiture équipée d'une alarme conduira un voleur à s'attaquer à un véhicule moins bien protégé, la vidéosurveillance pourrait avoir pour effet de déplacer une certaine forme de criminalité en d'autres lieux plutôt que de la réduire. Même si elle peut contribuer, à certains égards, à restaurer une forme de sécurité ponctuelle, la vidéosurveillance ne doit pas éclipser d'autres méthodes de prévention de la criminalité intervenant à d'autres niveaux.

Une incompatibilité résulterait par exemple de l'utilisation d'un système de vidéosurveillance, dont la finalité annoncée est la prévention des vols dans l'entreprise, afin de contrôler la productivité des employés.

3.1.1.2.6. Le but doit être non seulement spécifique mais aussi proportionnel

Enfin, le principe de finalité stipule encore que les images traitées, par rapport aux finalités clairement définies et légitimes, doivent être *adéquates, pertinentes et non excessives.* L'enregistrement doit ainsi se dérouler de telle sorte que des images superflues ne soient pas prises.

Ainsi, des caméras filmant la voie publique devront éviter que ne figurent dans leur champ des entrées ou des fenêtres de bâtiments privés. En outre, le nombre d'appareils d'enregistrement placés et leurs fonctionnalités, de même que la présence ou l'absence d'une fonction de suivi automatique, ne peuvent être excessifs en fonction des finalités poursuivies.
Conformément à ce principe, un système de vidéosurveillance ne devra permettre l'identification des personnes filmées que lorsqu'une telle identification est nécessaire à la réalisation de l'objectif poursuivi. Un système de contrôle de la fluidité du trafic routier devrait ainsi être installé de façon à filmer les personnes d'une distance suffisante afin de préserver leur anonymat.

3.1.1.2.7. Qu'en est-il des caméras qui filment des données sensibles?

Le fait de filmer des manifestations peut poser un problème à la lumière de la loi sur la vie privée qui protège spécifiquement certaines données sensibles[1]. Nous rappelons le principe de la loi, selon lequel le traitement de données sensibles est interdit sauf dans les cas précis, énumérés par la loi. La question se pose principalement dans le contexte de l'utilisation de caméras de vidéosurveillance dans des lieux publics ou accessibles au public.
Concrètement, cela signifie qu'il faut une loi pour filmer des manifestations en tant qu'autorité, ou pour filmer des cambrioleurs en tant que particulier. Ces lois n'existent pas. La Commission, qui est consciente du problème, ne le résout pas vraiment mais propose une solution intermédiaire.

1. Cf. les articles 6, 7 et 8 de la loi.

Primo, la Commission précise que toute information n'est pas forcément sensible en elle-même, ces caractéristiques pouvant résulter du contexte et des finalités pour lesquelles les données sont traitées[1].

Secundo, la Commission souligne néanmoins que la localisation de certaines caméras engendre davantage de risques que d'autres d'incitation à une déduction du caractère sensible des données filmées. Elle pense par exemple aux données filmées par une caméra ayant dans son champ le porche d'une église, l'entrée d'un syndicat, d'un hôpital ou encore l'entrée du cabinet d'un médecin spécialiste.

Au regard du principe de proportionnalité et des risques accrus d'atteinte à la vie privée des personnes concernées, le champ couvert par les caméras devrait limiter les possibilités d'identification des personnes visées.
Si la légitimité du traitement est admise lorsque son responsable se conforme à une disposition réglementaire et exécute une mission d'intérêt public[2], il s'agira en tout état de cause, conformément au principe de pertinence développé *supra*, de circonscrire le champ des caméras à ce qui est strictement nécessaire et indispensable à l'objectif poursuivi. En résumé, la Commission ne dit rien de plus que « d'être prudent avec les images dont on peut déduire des données sensibles ».

3.1.1.2.8. Combien de temps conserver les images?

Les risques d'atteinte à la vie privée sont d'autant plus importants que la durée de conservation des données est longue.
D'un point de vue technique, la durée de conservation des données dépend d'un facteur extérieur à la finalité du traitement, c'est-à-dire la qualité de la conservation dans le temps du support physique d'enregistrement[3].
Face aux progrès techniques qui permettent aujourd'hui la diminution des espaces nécessaires au stockage des données, il faut rappeler un principe essentiel de l'article 4 de la loi. Selon ce principe, *les données ne peuvent être conservées ou*

1. Ainsi, la couleur de la peau des personnes filmées, qu'elle soit blanche ou noire, ne peut être considérée comme sensible en elle-même, mais elle le serait si par exemple l'objectif de l'enregistrement d'images était d'identifier et de classer les personnes filmées selon leur couleur de peau.
2. Cf. article 6, 1 LVP.
3. On note à cet égard que l'usage de plus en plus répandu des techniques numériques permet actuellement la conservation des images sans entraîner les problèmes de stockage physique que présentaient les supports analogiques, ce qui constitue un risque supplémentaire de voir des données non pertinentes conservées « à toutes fins utiles ultérieures ».

traitées pour une durée excédant le temps nécessaire à la réalisation de la finalité poursuivie.

C'est le propriétaire de la caméra qui doit appliquer ce principe. La Commission prend l'exemple de l'enregistrement d'images dans un lieu public (jardin public, square, ...), la finalité de l'enregistrement étant de disposer d'éléments d'investigation en cas de constat visuel d'atteinte aux personnes ou aux biens. Si aucune infraction n'est constatée, les images ne devraient pas être conservées plus d'une demi-journée ou une journée avant d'être effacées (par exemple par surcharge).

Enfin, la Commission note que si les images ne sont pas du tout conservées, bien qu'il y ait malgré tout un traitement au sens de la loi, le risque d'atteinte à la vie privée est moindre. La Commission préconise de ce fait de limiter autant que possible la vidéosurveillance à une captation d'images sans conservation.

3.1.1.2.9. Droit d'accès, de rectification, de suppression et de non-utilisation

La LVP dispose en ses articles 10 et 12 que les personnes enregistrées ont le droit de prendre connaissance des données à caractère personnel les concernant, et d'exiger, le cas échéant, la rectification, la suppression ou la non-utilisation de ces données.

Ces articles ne trouvent bien entendu à s'appliquer que lorsque les données ont fait l'objet d'un enregistrement et d'une conservation. Dans son avis n° 14/95 du 7 juin 1995, la Commission avait considéré que s'il existait un index relatif à ces données à caractère personnel, donner suite à ces droits par le maître du traitement ne posait pas de problème sérieux. Dans le cas contraire, la Commission soulignait les difficultés de retrouver les images concernées.
L'évolution de la technique dans ce domaine et l'utilisation de plus en plus courante de procédés d'enregistrement numériques devraient aujourd'hui faciliter le repérage des séquences précises comportant l'image des personnes concernées.

La personne souhaitant avoir accès à ses données devrait accompagner sa demande d'indications suffisamment détaillées, afin de permettre la localisation précise de ses données sur l'enregistrement (date, heure et localisation exactes)[1]. Que la personne concernée souhaite ou non assister à la recherche et à la présentation des informa-

1. Les données communiquées à cet effet ne peuvent bien entendu être utilisées à des fins différentes de l'accès de la personne à ses données, ni être conservées pour une durée supérieure à l'exercice de ce droit d'accès.

tions la concernant, cette recherche devrait en outre être effectuée par le responsable du traitement ou l'un de ses gestionnaires. Ces différentes garanties sont indispensables à la protection de la vie privée des tiers qui apparaîtraient sur le film[1].

3.1.1.2.10. Les caméras doivent être déclarées

Le traitement de données à caractère personnel sous la forme d'images doit être préalablement déclaré à la Commission, en vue de son enregistrement dans le registre public des traitements automatisés.

La loi précise que la déclaration doit être faite préalablement à la mise en œuvre d'un traitement de données à caractère personnel, et ce, sous peine d'amende de cent francs à cent mille francs, conformément à l'article 39, 7° de la loi. Traiter des données à caractère personnel sans avoir déclaré le traitement (en temps voulu) est un fait punissable.

La déclaration doit être effectuée, qu'il y ait ou non conservation des données. L'absence de conservation des données étant toutefois un élément important au regard de l'impact du traitement en matière de protection de la vie privée, cette information devrait être mentionnée dans le cadre de la déclaration.

Enfin, il convient de remarquer qu'il faut satisfaire à l'obligation de déclaration, aux termes de l'article 17 de la loi, par (finalité de) traitement. Ce critère de finalité[2] ne dépend dès lors pas d'autres facteurs tels que l'éventuelle organisation territoriale d'une entreprise ou le nombre de caméras installées dans une entreprise. En d'autres termes, il ne faut pas satisfaire à l'obligation de déclaration autant de fois qu'il y a de caméras installées, mais bien autant de fois qu'il y a de finalités ou de traitements distincts.

---

1. La Commission ajoute ce qui suit: *« Si une réglementation à venir devait considérer, comme la directive européenne 95/46 en prévoit la possibilité, que la protection des droits et libertés d'autrui constitue une exception au droit d'accès, la Commission préconise qu'un mode d'accès alternatif aux données soit envisagé. La Commission pourrait ainsi sur la base de renseignements suffisamment détaillés effectuer un accès indirect au nom du demandeur ».*
2. Cf. à ce propos le rapport Merckx-Van Goey, p. 80 et l'avis de la Commission n° 10/92 du 20 août 1992 concernant le projet de loi relatif à la protection de la vie privée à l'égard des traitements de données à caractère personnel, tel que transmis par la Chambre des Représentants au Sénat.

3.1.1.2.11. Sécurité du traitement

Le développement actuel des modes d'enregistrement numériques permet une manipulation des images difficilement envisageable dans le cadre d'un traitement analogique des données. Par des traitements consécutifs de l'enregistrement, il devient ici aisé de constituer non seulement des fichiers d'images, mais également des fichiers d'informations dérivées, permettant des analyses, des recoupements a posteriori, ainsi qu'une analyse d'une séquence d'images, appartenant à la même prise de vue ou à des prises de vues distinctes.
De telles possibilités de manipulation des images engendrent des risques de falsification des informations, auxquels tout responsable de traitement est tenu de faire face en vérifiant l'exactitude des données traitées et en prenant toutes les mesures de sécurité adéquates (article 16)[1].

Ces mesures de sécurité doivent également viser à prévenir tout autre risque d'atteinte aux données tel que leur vol, leur effacement, etc., ainsi que tout risque d'utilisation pour d'autres finalités.

La Commission estime en outre qu'il est indispensable que le mode d'enregistrement et de conservation soit explicitement précisé dans les déclarations de traitement relatif aux images, pour qu'elle dispose de tous les éléments utiles à son appréciation du traitement.

3.1.1.2.12. La Commission plaide également pour une loi sur l'utilisation des caméras

Tout au long de son dernier avis, la Commission insiste sur la nécessité de créer une législation plus claire sur les caméras. Elle indique ce faisant que les principes cités ci-dessus ne constituent que des normes minimales. Il est vrai qu'il s'agit de normes indispensables qui devraient être respectées par chacun lors de la mise en service de systèmes de vidéosurveillance. Par ailleurs, toute initiative visant à réglementer la vidéosurveillance devrait en tenir compte. La Commission souhaite être consultée dans le cadre de la rédaction de tout texte normatif en la matière, en ce compris les arrêtés d'exécution éventuels, qui pourrait par exemple porter sur l'application de la vidéosurveillance dans des secteurs plus spécifiques. Dans ce qui suit, nous examinerons comment la Commission applique ces principes à la problématique des caméras dans les immeubles à appartements. Ensuite, nous aborderons quelques autres problèmes pratiques.

---

1. Telles que le cryptage des données, un accès conditionné par un mot de passe, etc.

3.1.2. Cas particuliers d'utilisation de caméras

3.1.2.1. Systèmes de caméras dans les immeubles à appartements

3.1.2.1.1. Introduction

Peu après l'avis que nous venons de commenter, la Commission a rendu un deuxième avis, plus spécifique, relatif cette fois à l'utilisation de systèmes de vidéosurveillance dans les halls d'immeubles à appartements[1]. L'origine de cet avis a été le nombre croissant de questions adressées à la Commission en ce qui concerne l'utilisation de caméras dans le hall d'un immeuble à appartements.

La Commission souligne que la loi s'applique à l'utilisation de caméras de vidéosurveillance dès lors que les images filmées se rapportent à une ou plusieurs personnes identifiées ou identifiables, que les images soient ou non conservées (article 1er, § 2 et article 3). Les principes analysés dans le cadre de l'avis n° 34/99 s'appliquent incontestablement aux systèmes de vidéosurveillance utilisés dans le hall d'un immeuble à appartements.

3.1.2.1.2. Obligation d'information

En vertu de l'article 9 de la loi, le responsable du traitement de données a l'obligation d'informer les personnes filmées des éléments suivants:
– le nom et l'adresse du responsable du traitement ou son représentant,
– les finalités du traitement,
– l'existence d'un droit d'accès et de rectification des personnes concernées,
– les destinataires ou les catégories de destinataires des données.

Un avis lisible comportant les informations mentionnées ci-dessus doit à cet effet être placé bien en évidence dans le hall d'entrée afin d'être aperçu depuis le seuil du bâtiment.

3.1.2.1.3. Formulation claire de l'objectif des caméras

La finalité de la caméra doit être clairement définie. L'utilisation de caméras dans le hall d'un immeuble aura généralement pour finalité la protection contre les atteintes aux biens et aux personnes. Cette finalité devra être formulée clairement dans l'avis informatif placé dans le hall de l'immeuble.

---

1. Commission de la protection de la vie privée, avis n° 03/2000 du 10 janvier 2000 relatif à l'utilisation de systèmes de vidéosurveillance dans les halls d'immeubles à appartements.

3.1.2.1.4. Réfléchir et se concerter avec tous les habitants avant de placer une caméra

La finalité du traitement doit être légitime. En vertu du *principe de proportionnalité*, l'intérêt général ou les intérêts légitimes du gestionnaire du traitement doivent être mis en balance avec le droit à la protection de la vie privée de la personne enregistrée.

Dans l'hypothèse de l'utilisation de caméras dans le hall d'un immeuble, les intérêts en jeu sont, d'une part, la sécurité des personnes habitant l'immeuble et de leurs biens, ainsi que la sécurité des visiteurs et, d'autre part, le respect de la vie privée des personnes habitant l'immeuble ainsi que celle des visiteurs. La Commission s'est prononcée dans son avis n° 34/99 pour une appréciation stricte du respect du critère de proportionnalité lorsque l'utilisation de systèmes de vidéosurveillance est effectuée dans des lieux non accessibles au public. Elle demandait notamment que le consentement des personnes concernées soit pris en considération pour une telle appréciation.

Si, dans le cas d'espèce, le hall d'un immeuble ne peut être considéré comme un lieu non accessible au public, sa fonction de « sas » d'accès à un lieu privé requiert néanmoins que des garanties suffisantes soient adoptées. Ainsi, l'assentiment des personnes habitant l'immeuble devrait être recueilli par exemple par le biais d'un vote conforme au règlement de l'assemblée des copropriétaires et/ou des colocataires.

Lors de l'examen de la légitimité du traitement de données envisagé, il ne faudra pas perdre de vue que celui-ci doit être un *moyen adéquat et nécessaire* à la réalisation de l'objectif poursuivi.
Ce moyen ne pourra en outre être retenu *que* si d'autres mesures moins attentatoires à la vie privée, telles que dans le cas d'espèce, des verrouillages complémentaires, le renforcement des portes d'entrée, des systèmes d'alarme, s'avèrent *insuffisantes ou impraticables*.

3.1.2.1.5. Quelles images et quelle utilisation?

Les images filmées doivent être adéquates, pertinentes et non excessives par rapport à la finalité poursuivie. L'installation d'une caméra dans le hall d'entrée d'un immeuble devra être effectuée de façon à ce que n'entrent dans son champ que les images strictement nécessaires à la surveillance envisagée.

Il semble donc superflu et non pertinent que le champ de la caméra couvre par exemple le tableau des interphones ou l'entrée des appartements privés. De façon générale, la caméra devrait être dirigée vers la porte d'entrée principale du bâtiment et en aucun cas être positionnée de façon à ce qu'il soit possible de déterminer vers quel appartement se dirige la personne qui entre dans le hall.

Les images ne peuvent en outre être utilisées que dans le cadre de la finalité déclarée et ne peuvent donner lieu à d'autres utilisations. Les images de caméras de sécurité ne peuvent tendre à satisfaire la curiosité de certaines personnes.

3.1.2.1.6. Durée et modalités de conservation des images

En vertu du principe selon lequel *les données ne peuvent être conservées pour une durée excédant le temps nécessaire à la réalisation de la finalité poursuivie*, les données enregistrées par une caméra située dans le hall d'un immeuble devraient être effacées dans un délai particulièrement bref.

Comme la constatation d'une infraction aux biens ou aux personnes dans un immeuble à appartements aura lieu dans la plupart des cas dans les heures qui suivent sa perpétration, il semble qu'un délai de conservation des données de 24 heures ou de 48 heures paraisse suffisant au regard de la finalité poursuivie dans la mesure où aucune atteinte aux biens ou aux personnes n'a été constatée dans ce délai.

Les données doivent par ailleurs être conservées par une personne déterminée[1], et ne doivent pas être accessibles aux tiers en dehors des possibilités prévues par la loi en matière de droit d'accès de toute personne à ses propres données[2].

1. Ayant les compétences techniques nécessaires afin de permettre notamment un accès spécifique des personnes concernées à leurs données à caractère personnel.
2. Articles 10 et 12 de la loi. Voir supra dans l'avis n° 34/99 de la Commission pour plus de détails sur cette question ainsi que sur les obligations à respecter en matière de sécurité des données.

3.1.2.2. Caméras de surveillance et législation sur le droit collectif du travail

3.1.2.2.1 Introduction – conventions collectives concernées

Sur le plan du droit du travail, différentes lois ont un impact au moins indirect dans le domaine de la surveillance visuelle[1].
Les compétences des conseils d'entreprise sont énumérées dans la loi de 1948 portant organisation de l'économie[2]. Les conseils d'entreprise ont pour mission de donner leur avis et de formuler toutes suggestions ou objections sur toutes mesures qui pourraient modifier l'organisation du travail, les conditions de travail et le rendement de l'entreprise (article 15a L. 1948). Comme les techniques de contrôle (par ex. contrôle par caméras) influencent les conditions de travail dans une entreprise, le conseil d'entreprise doit être consulté au préalable, avant que les circuits de télévision soient installés.

L'implication du conseil d'entreprise dans les modifications des conditions de travail a notamment été confirmée par une convention collective de travail de 1972, à savoir la C.C.T. n° 9[3]. Pour permettre au conseil d'entreprise d'accomplir les missions qui lui sont confiées par l'article 15a de la loi du 20 septembre 1948, il sera informé des projets et mesures susceptibles de modifier les circonstances et les conditions dans lesquelles s'exécute le travail dans l'entreprise ou dans une de ses divisions

1. Cf. DELARUE, R., « Bescherming van de privacy in de onderneming en de begrenzing van de patronale prerogatieven », *Soc. Kron*., 1992, 4, 133-141; DE HERT, P., « Oude en nieuwe wetgeving op controletechnieken in bedrijven », *Soc. Kron*., 1995, n° 3, 105-118; DE SCHUTTER, O., « La vidéosurveillance et le droit au respect de la vie privée », *Journ. procès*, n° 300, 8 mars 1996, 20.
2. Loi du 20 septembre 1948 portant organisation de l'économie, *M.B.,* 27-28 septembre 1948.
3. C.C.T. n° 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise conclus au sein du Conseil national du travail, rendue obligatoire par A.R. du 12 septembre 1972*, M.B.,* 25 novembre 1972 et concernant l'article 10 de la C.C.T. complétée par la C.C.T. n° 34 du 27 février 1981, rendue obligatoire par A.R. du 21 septembre 1981, *M.B*., 6 octobre 1981, err. *M.B.,* 4 décembre 1981.

(article 10 C.C.T. 9)[1]. Selon le commentaire de la C.C.T. 9, il est en effet évident que le texte de l'article 15a de la loi de 1948 précité implique que le conseil d'entreprise a le droit de donner son avis et de formuler toutes suggestions ou objections sur toutes mesures qui pourraient modifier l'organisation du travail, les conditions de travail et le rendement de l'entreprise (commentaire de l'article 10 C.C.T. 9).

La loi de 1948 et la C.C.T. n° 9 couplent des sanctions pénales au non- respect des procédures de concertation. L'employeur qui met obstacle au fonctionnement du conseil d'entreprise, tel qu'il est prévu dans cette loi, ses arrêtés d'exécution et les conventions collectives de travail rendues obligatoires par le Roi est passible d'une amende (article 32, 2° Loi 1948). Une même amende est prévue pour l'employeur qui entrave l'exercice des missions du conseil d'entreprise notamment en ne fournissant pas les renseignements prévus par la loi, ses arrêtés d'exécution ou les conventions collectives de travail rendues obligatoires par le Roi ou en ne les fournissant pas selon les règles prévues ou en ne procédant pas aux consultations selon les règles prévues (article 32, 3°, Loi 1948). Les chefs d'entreprise sont civilement responsables du paiement des amendes prononcées à charge de leurs directeurs, gérants ou préposés à la surveillance ou à la direction (article 34, Loi 1948).

Il faut également mentionner la C.C.T. n° 39. La convention collective de travail n° 39 concernant l'information et la coopération sur les conséquences sociales de l'introduction des nouvelles technologies date de 1983[2]. Aux termes de cette convention, l'employeur doit respecter une procédure d'information et de consultation lors de l'introduction dans l'entreprise de technologie qui a des 'conséquences sociales importantes'. *« Lorsque l'employeur a décidé d'un investissement dans une nouvelle technologie et lorsque celui-ci a des conséquences collectives importantes en ce qui concerne l'emploi, l'organisation du travail ou les conditions de travail, il*

---

1. *Les informations prévues (...) par cette convention doivent se rapporter à des mesures de caractère collectif qui viendraient à modifier les circonstances et conditions de travail. Quand ces mesures s'appliquent à un nombre limité de travailleurs, voire à des travailleurs individuels, ceux-ci seront préalablement informés et consultés. Ils peuvent se faire assister, à leur demande, par un délégué syndical. Les mesures dont il est question ci-dessus comprendront entre autres: (...) les modifications de l'environnement matériel et humain (exemple : implantation de machines modifiant les conditions de travail...); (...) les changements dans les méthodes de fabrication et de travail* (commentaire de l'article 10 C.C.T. 9). Le fait que ces systèmes de surveillance par caméras modifient l'environnement matériel et humain semble difficile à réfuter. Le conseil d'entreprise est donc également compétent. En vertu de la C.C.T. 9, le conseil d'entreprise doit être préalablement consulté.
2. C.C.T. n° 39 C.N.T. du 13 décembre 1983 concernant l'information et la coopération sur les conséquences sociales de l'introduction des nouvelles technologies, rendue obligatoire par A.R. du 25 janvier 1984, *M.B.,* 8 février 1984.

est tenu, au plus tard trois mois avant le début de l'implantation de la nouvelle technologie, d'une part de fournir une information écrite sur la nature de la nouvelle technologie, sur les facteurs qui justifient son introduction ainsi que sur la nature des conséquences sociales qu'elle entraîne et d'autre part, de procéder à une concertation avec les représentants des travailleurs sur les conséquences sociales de l'introduction de la nouvelle technologie »[1]. Pour la C.C.T., le contrôle ne peut donc pas être la raison principale mais en fait néanmoins partie. Le texte est en effet très clair et il n'y a que peu de doutes en ce qui concerne son application à la surveillance par caméras orientées sur le personnel. La convention n'est toutefois applicable qu'aux entreprises qui comptent au moins cinquante travailleurs, ce qui exclut les entreprises plus petites. Les règlements de travail, au contraire, doivent être établis dans toutes les entreprises et ceci avec la collaboration des travailleurs sous peine de sanctions pénales.
Mentionnons enfin la loi instituant les règlements de travail. Dans leur forme actuelle, les deuxièmement et cinquièmement de l'article 6 de la loi du 8 avril 1965 instituant les règlements de travail stipulent: *« Le règlement de travail doit indiquer: 2° les modes de mesurage et de contrôle du travail en vue de déterminer la rémunération; (...) 5° les droits et obligations du personnel de surveillance »*. On peut déduire de cette disposition que les techniques de contrôle visuelles ne peuvent en principe pas être introduites dans une entreprise sans avoir été au préalable annoncées dans le règlement de travail[2].

3.1.2.2.2. L'objectif de la Convention collective de travail n° 68

La réglementation que nous venons d'évoquer n'est cependant que rarement appliquée dans la pratique[3]. Il s'agit pourtant de lois dont les dispositions sont formulées de manière générale et ne laissent aucun doute sur le fait qu'elles sont applicables à la matière en question. Il faut donc une réglementation complémentaire pour souligner l'existence et la pertinence de ce cadre légal et en même temps pour renforcer

1. Art. 2 § 1er. C.C.T. 39.
2. DE SCHUTTER, O., « La vidéosurveillance et le droit au respect de la vie privée », *Journal des Procès*, 1996, n° 298, 16.
3. Non seulement la loi instituant les règlements de travail n'est pas suffisamment respectée, mais la surveillance est de plus en plus souvent confiée à des entreprises de gardiennage ou à des cellules de sécurité spécialisée de l'entreprise. Ce sont en fait des nouveaux venus sur le marché du travail. Ils sont le produit d'une nouvelle mentalité et ne connaissent généralement pas les prescriptions en matière de droit du travail. La concertation et l'information sur la surveillance sont perçues comme une atteinte aux propres prérogatives, comme une ingérence dans leur job. On ne tient relativement compte que du Code pénal et de la loi sur la fonction de police; le droit du travail est ignoré (DE HERT, P., *l.c.,* 117).

ce cadre. Nous avons déjà écrit précédemment que l'on pouvait songer à regrouper toutes les lignes de force et les règles relatives à la surveillance dans une nouvelle convention de travail centrale ou dans d'autres instruments de droit du travail. En 1998, le Conseil National a conclu une C.C.T. relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail[1]. Cette convention a pour but de garantir le respect de la vie privée des travailleurs dans l'entreprise et la protection de leur dignité ainsi que de préserver le droit fondamental à cet égard en définissant, compte tenu des nécessités d'un bon fonctionnement de l'entreprise, pour quelles finalités et à quelles conditions la surveillance par caméras sur le lieu de travail, avec ou sans conservation des images, peut être introduite[2].

Lors de la rédaction du texte, le Conseil National du Travail s'est inspiré des réglementations existantes en matière de surveillance par caméras dans le contexte du droit du travail[3]. La C.C.T. décrit ce qu'il faut entendre par surveillance par caméras sur le lieu de travail, à quelles conditions cette surveillance est autorisée et quelles sont les prescriptions à respecter en la matière. Son but est également de concrétiser le contenu de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard du traitement de données à caractère personnel, en ce qui concerne la surveillance par caméras. La convention confirme et concrétise les principes de la loi sur la vie privée, notamment le principe de finalité, le principe de proportionnalité

1. Arrêté royal du 20 septembre 1998 rendant obligatoire la convention collective de travail n° 68 conclue le 16 juin 1998 au sein du Conseil National du Travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, *M.B.,* 2 octobre 1998.
2. Cf. art.1er C.C.T. n° 68.
3. Hormis les lois commentées ci-dessus relatives au droit collectif du travail, le C.N.T. renvoie aux instruments juridiques suivants comme ayant servi de fil conducteur à la rédaction de la C.C.T.: le traité n° 108 du Conseil de l'Europe du 28 janvier 1981 la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, ratifié par la Belgique par la Loi du 17 juin 1991; la recommandation n° R(89)2 du Comité des ministres du Conseil de l'Europe « sur la protection des données à caractère personnel utilisées à des fins d'emploi », qui précise les principes du traité précédent dans le contexte de droit du travail; la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données; le code de conduite relatif à la protection des données à caractère personnel des travailleurs adopté par le Conseil d'administration de l'AIT au cours de sa 267e session de novembre 1996 et à laquelle le C.N.T. collaboré dès la phase préparatoire, ce qui a mené à son avis n° 1.160 du 23 juillet 1996; l'article 22 de la Constitution belge qui reconnaît le droit au respect de la vie privée; la Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel; l'avis n° 14/95 du 7 juin 1995 concernant l'applicabilité de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel aux enregistrements d'images et leurs conséquences. Nous reviendrons plus loin sur certains de ces instruments.

et l'obligation d'information, par rapport au lieu de travail. La convention collective de travail veut également tenir compte des dispositions légales et conventionnelles en matière d'information et de consultation des représentants des travailleurs[1].

3.1.2.2.3 Le contenu de la Convention collective de travail n° 68

L'article 2 donne la définition suivante de ce qu'il y a lieu d'entendre par surveillance par caméras: *« Pour l'application de la présente convention collective de travail, il y a lieu d'entendre par surveillance par caméras, tout système de surveillance comportant une ou plusieurs caméras et visant à surveiller certains endroits ou certaines activités sur le lieu de travail à partir d'un point qui s'en trouve géographiquement éloigné dans le but ou non de conserver les images dont il assure la collecte et la transmission ».*

Conformément à l'article 5 de la LVP[2], la C.C.T. donne un aperçu des finalités pour lesquelles la surveillance par caméras est autorisée. Selon la C.C.T., la surveillance par caméras sur le lieu de travail n'est autorisée que lorsque l'une des finalités suivantes est poursuivie[3]:

1° la sécurité et la santé;
2° la protection des biens de l'entreprise;
3° le contrôle du processus de production[4];
4° le contrôle du travail du travailleur

L'employeur doit définir clairement et de manière explicite la finalité de la surveillance par caméras[5]. Le commentaire ajouté à cette disposition de la C.C.T. montre également que l'utilisation des caméras à des fins de formation est autorisée, étant donné qu'il ne s'agit pas de surveillance. Selon le commentaire, en cas de surveillance secrète par caméras, les dispositions du Code pénal s'appliquent et cette forme de surveillance ne peut être introduite qu'en conformité avec les prescriptions du Code d'instruction criminelle. Cela signifie donc que les employeurs ne sont pas

1. Commentaire de l'art. 1er C.C.T. n° 68.
2. L'article 5 de la LVP stipule en effet que les données à caractère personnel ne peuvent être traitées que pour des finalités déterminées et légitimes.
3. Art. 4§ 1 de la CCT n°68
4. Le contrôle du processus de production peut porter tant sur les machines que sur les travailleurs. Si le contrôle porte uniquement sur les machines, il a pour but d'en vérifier le bon fonctionnement. Si le contrôle porte sur les travailleurs, il a pour but l'évaluation et l'amélioration de l'organisation du travail.
5. Art. 4 § 2 C.C.T. n° 68.

autorisés à filmer en secret. Dans les cas où cela semble nécessaire, à savoir lorsqu'il y a suspicion d'activités criminelles, il y a lieu de faire appel aux autorités publiques[1].

La C.C.T. distingue clairement la surveillance par caméras permanente et temporaire[2]. Il faut également distinguer les finalités pour lesquelles on recourt à la surveillance permanente et/ou temporaire. La surveillance par caméras permanente ou temporaire est autorisée en vue d'assurer la sécurité et la santé, la protection des biens de l'entreprise et de permettre le contrôle du processus de production qui porte uniquement sur les machines (art. 6, al. 2).

La surveillance par caméras ne peut être que temporaire si elle vise le contrôle du processus de production qui porte sur les travailleurs et en cas de contrôle du travail du travailleur (art. 6, al. 3). Le commentaire de l'article précise que la surveillance par caméras permanente des machines n'est autorisée que dans la mesure où le but n'est pas de viser le travailleur.

Outre la description des finalités, la convention accorde également de l'attention à la concrétisation du principe de proportionnalité. En se rapprochant fortement des termes de l'article 5 de la loi du 8 décembre 1992, il est dit que l'employeur ne peut utiliser la surveillance par caméras d'une manière incompatible avec la finalité expressément décrite (art. 7, al. 1er). Cela implique par exemple que les images prises en vue de prévenir ou de constater des infractions en matière de sécurité, ne peuvent pas être utilisées pour analyser les comportements d'une personne ou comme horloge pointeuse déguisée. La surveillance par caméras doit être adéquate, pertinente et non excessive au regard de cette finalité (art. 7, al. 2). Cela signifie notamment que la prise de vues doit se faire en telle manière que des images superflues ne sont pas réalisées inutilement.

Par principe, l'article 8 de la C.C.T. stipule que la surveillance par caméras ne peut entraîner une ingérence dans la vie privée du travailleur. Si toutefois la surveillance par caméras entraîne une ingérence dans la vie privée du travailleur, cette ingérence

---

1. Cf. le commentaire de l'art. 4 C.C.T. n° 68: *« La présente convention collective de travail laisse en l'état la possibilité d'utiliser des caméras à des fins de formation étant donné qu'il ne s'agit pas de surveillance »*.
2. Les deux notions sont définies à l'art. 5 C.C.T. n° 68: *« La surveillance par caméras est permanente lorsque la ou les caméras fonctionnent en permanence. La surveillance par caméras est temporaire lorsque la ou les caméras sont installées soit à titre temporaire soit de manière fixe mais ne fonctionnent que pendant une ou plusieurs périodes »*. La littérature souligne que le manque de précision de ces définitions constitue le principal point faible de la C.C.T.

doit être réduite à un minimum, selon la procédure fixée aux articles 10 et 11 (infra) (art. 8). Tout compte fait, la C.C.T. comporte trois types de conditions de procédure. Un aperçu.

3.1.2.2.4. Conditions de procédure qui doivent toujours être respectées

Préalablement et lors de la mise en œuvre de la surveillance par caméras, l'employeur doit informer le Conseil d'entreprise sur tous les aspects de la surveillance par caméras visés au § 4, conformément aux dispositions de la convention collective de travail n° 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise conclus au sein du Conseil National du Travail[1].
A défaut de Conseil d'entreprise, cette information est fournie au Comité pour la prévention et la protection au travail ou, à défaut d'un tel Comité, à la délégation syndicale ou, à défaut, aux travailleurs[2].

Lors de la mise en œuvre de la surveillance par caméras, l'employeur doit informer les travailleurs concernés sur tous les aspects de la surveillance par caméras et porte 'au moins' sur les aspects suivants de la surveillance par caméras:
– la finalité poursuivie;
– le fait que des images sont ou non conservées;
– le nombre de caméras et l'emplacement de la ou des caméras;
– la ou les périodes concernées pendant lesquelles la ou les caméras fonctionnent[3].

Cette obligation d'information a pour but d'accroître la transparence en matière de surveillance par caméras et de permettre un dialogue afin que l'introduction de cette surveillance puisse se faire dans un climat de confiance[4].

3.1.2.2.5. Conditions de procédure qui doivent être respectées en cas de contrôle du travail

Le contrôle du travail du travailleur est l'une des quatre finalités admises en vertu de l'article 4 de la C.C.T. qui ajoute immédiatement que cela doit se faire conformément à l'article 9, § 2 de la C.C.T. L'article 4 mentionne encore que la poursuite de

1. Art. 9 § 1er. C.C.T. n° 68.
2. Art. 9 § 1er. C.C.T. n° 68.
3. Art. 9 § 3 *juncto* § 4. C.C.T. n° 68.
4. Commentaire de l'art. 9 C.C.T. n° 68.

cette finalité ne peut avoir pour conséquence que les décisions et évaluations de l'employeur se fondent exclusivement sur les données collectées par voie de surveillance par caméras.

Lorsque la surveillance par caméras a pour objet le contrôle des prestations de travail, et plus particulièrement le mesurage et le contrôle en vue de déterminer la rémunération ou a des implications sur les droits et obligations du personnel de surveillance, l'employeur applique la procédure 'minimale' d'information décrite ci-dessus, mais il fournit cette information dans le cadre de la procédure fixée aux articles 11 et suivants de la loi du 8 avril 1965 instituant les règlements de travail[1].

En effet, dans le cas spécifique du mesurage et du contrôle en vue de déterminer la rémunération ou les implications sur les droits et obligations du personnel de surveillance, des règles spécifiques s'appliquent en vertu de la loi du 8 avril 1965 instituant les règlements de travail. Le travailleur peut notamment prendre connaissance en permanence et sans intermédiaire – sans préjudice du droit à l'assistance de son délégué syndical – du règlement de travail et de ses modifications. L'employeur lui en remet, en outre, une copie[2].

3.1.2.2.6. Conditions de procédure qui doivent être respectées en cas d'ingérence dans la vie privée

Les articles 10 et 11 de la convention traitent de l'obligation de consultation. Ceux-ci complètent la procédure d'information au cas où, conformément à l'article 8 de la C.C.T., il est question d'une ingérence dans la vie privée du travailleur ce qui doit en principe être évité ou limité à un minimum.
Si, à l'occasion de l'information, il apparaît que la surveillance par caméras peut avoir des implications sur la vie privée d'un ou de plusieurs travailleurs, le Conseil d'entreprise ou, à défaut, le Comité pour la prévention et la protection au travail examine les mesures qu'il y a lieu de prendre pour réduire l'ingérence dans la vie privée à un minimum (art. 10, § 1er).

Si la surveillance par caméras est introduite en vue du contrôle du processus de production qui porte sur les travailleurs ou en vue du contrôle du travail du travailleur – dans ces cas la surveillance par caméras peut tout au plus être temporaire – cet examen est également effectué par le conseil d'entreprise ou de comité pour la préven-

1. Art. 9 § 2. C.C.T. n° 68.
2. Commentaire de l'art. 9 C.C.T. n° 68.

tion et la protection au travail. A défaut de ces organes, l'examen est effectué d'un commun accord entre l'employeur et la délégation syndicale (art. 10, § 2).

Le Conseil d'entreprise ou, à défaut, le Comité pour la prévention et la protection au travail doit en outre évaluer régulièrement les systèmes de surveillance utilisés et faire des propositions en vue de les revoir en fonction des développements technologiques[1].

Implications

– lorsque les caméras ne constituent pas une ingérence dans la vie privée, une procédure d'information doit seule être suivie et pas de procédure de consultation;

– lorsque les caméras constituent une ingérence dans la vie privée, les deux procédures doivent être suivies;

– lorsqu'il n'y a ni conseil d'entreprise ni comité pour la prévention et la protection, la délégation syndicale est toujours informée;

– lorsque les caméras constituent une ingérence dans la vie privée et qu'il n'y a ni conseil d'entreprise ni comité pour la prévention et la protection, la délégation syndicale n'est impliquée *que* dans la procédure de consultation lorsque celle-ci porte sur le fait de filmer des personnes et doit en d'autres termes être temporaire;

– on n'a pas pensé à conférer, dans ces cas, une compétence de réévaluation régulière à la délégation syndicale, compétence que le conseil d'entreprise ou le comité pour la prévention et la protection ont pourtant;

– la C.C.T. ne mentionne pas la C.C.T. n° 39. Rappelons que, selon cette convention, l'employeur doit respecter une procédure d'information et de concertation lors de l'introduction dans l'entreprise de technologie qui a des « conséquences collectives importantes ». Cette procédure stricte n'est par conséquent pas applicable lorsqu'une entreprise procède à de la surveillance par caméras;

– contrairement à la C.C.T. n° 39 relative aux nouvelles technologies[2], cette convention est applicable à toutes les entreprises qui placent des caméras. Cette

1. Art. 11 C.C.T. n° 68.
2. Cette C.C.T. n'est applicable qu'aux entreprises qui occupent au moins 50 travailleurs.

convention est en outre axée explicitement sur la surveillance, en l'occurrence la surveillance par caméras sur le lieu de travail, alors que le contrôle n'était pas le but principal de la C.C.T. n° 39.

3.1.2.2.7. Obligations complémentaires de l'employeur lors de prises de vues

En ce qui concerne spécialement la surveillance par caméras avec conservation des images, la C.C.T. stipule que l'employeur doit traiter les images collectées de bonne foi et en conformité avec la finalité décrite[1].

De même, la C.C.T. stipule que si les images collectées sont utilisées à des finalités autres que celle pour laquelle la surveillance par caméras a été introduite, l'employeur doit s'assurer que cet usage est compatible avec la finalité initiale et prendre toutes les mesures pour éviter, vu le contexte, les erreurs d'interprétation[2].

3.1.2.2.8. Droits complémentaires des travailleurs lors de prises de vues

De façon un peu superflue, la C.C.T. stipule que, en cas d'utilisation de caméras avec prises de vues, les travailleurs peuvent à tout moment invoquer les dispositions des articles 10, 12 et 13 de la LVP[3], en d'autres termes les droits de consultation, de rectification et de s'adresser à la Commission de la protection de la vie privée.

« Superflue » ..., en effet puisque le droit de consultation est, par exemple, également possible en vertu de la LVP lorsqu'il n'y a pas de prise de vue. Dans ce cas, l'exercice du droit porte sur le contrôle de la position de la caméra. De même, on peut toujours recourir à la Commission, *même* en cas de surveillance par caméras sans prises de vues.

La C.C.T. est intéressante en ce qu'elle stipule que, pour exercer « ces » droits, les travailleurs ont le droit de se faire assister par leur délégué syndical[4]. Cette assistance fait défaut dans la LVP et peut être considérée comme un complément intéressant. Au sens strict, ce droit est cependant *uniquement* accordé en cas de surveillance par caméras avec prises de vues. Il va toutefois de soi que, dans l'esprit

1. Art. 12 *juncto* 13 § 1er C.C.T. n° 68.
2. Art. 12 *juncto* 13 § 2 C.C.T. n° 68.
3. Art. 12 *juncto* 14, premier alinéa C.C.T. n° 68.
4. Art. 12 *juncto* 14, deuxième alinéa C.C.T. n° 68.

de la C.C.T. et à la lumière de l'engagement de bonne foi, il faut également penser à ce droit à l'assistance en cas de plaintes ou de demandes relatives à la surveillance par caméras *sans* prises de vues.

3.1.2.2.9. La position de la cour de Cassation quant à l'irrégularité d'une preuve obtenue via le placement d'une caméra de surveillance sur les lieux de travail sans respect des formes prescrites

Introduction

Il est intéressant de confronter la réglementation développée par le biais des conventions collectives de travail (voir infra) avec la jurisprudence de la Cour de cassation relative à l'admission de certaines preuves, même recueillies irrégulièrement. En effet, plusieurs arrêts de la cour de cassation admettent la preuve recueillie par des caméras de surveillance sur les lieux de travail, alors que celles-ci ne respectent pas les principes énoncés ci-avant.

Position de la Cour de cassation en matière de preuve obtenue de manière illicite

Depuis 2003, la jurisprudence de la Cour de Cassation a connu une évolution importante en matière de sanction de la preuve obtenue de manière illicite[1].

Traditionnellement, le juge ne pouvait pas former sa conviction sur la culpabilité d'un prévenu sur base d'une preuve illicite[2].

Cette règle a été une première fois nuancée par la Cour de cassation dans un arrêt du 14 octobre 2003 selon lequel la circonstance qu'un élément de preuve a été obtenu illicitement n'entraînait pas ispo facto l'exclusion de celui-ci. Tel ne serait le cas que:
– lorsqu'une règle de forme prescrite à peine de nullité a été violée;
– lorsque l'irrégularité commise a entaché la fiabilité de la preuve;
– ou lorsque l'usage de la preuve est contraire au droit à un procès équitable.

1. Note de du Ministère Public à la Cour de Cassation Vandermeersch, sous Cass, 2 mars 2005 (disponible via le site www.juridat.be)
2. C'est-à-dire une preuve recueillie par un acte interdit par la loi, soit par un acte inconciliable avec les règles substantielles régissant la procédure pénale ou avec les principes généraux du droit (Cass., 13 mai 1986, Rev. dr. pén. crim., 1986, 905 avec les conclusions du procureur général Dujardin.

Dans un arrêt du 23 mars 2004, la Cour de cassation a adopté le même point de vue en y apportant des précisions. Elle énonce d'abord qu'en vertu du droit belge, l'utilisation d'une preuve n'est, en principe, pas autorisée lorsque cette preuve a été obtenue par l'autorité chargée de la recherche, de l'instruction ou de la poursuite d'une infraction ou par un dénonciateur, en méconnaissance d'une règle de procédure pénale suite à la violation du droit à la vie privée, des droits de la défense ou du droit à la dignité humaine.

En dehors des trois hypothèses citées ci-dessus, le juge doit apprécier l'admissibilité de la preuve à la lumière des articles 6 C.E.D.H. et 14 du Pacte international relatif aux droits civils et politiques, en tenant compte des éléments de la cause prise dans son ensemble, en ce compris la manière dont la preuve a été obtenue et les circonstances dans lesquelles l'irrégularité a été commise[1].

Dans un troisième arrêt du 16 novembre 2004, la Cour de Cassation a précisé qu'il ne résultait ni de l'article 6 de la Convention européenne des droits de l'homme et des libertés fondamentales, qui garantit un procès équitable, ni de l'article 8 de cette convention qui consacre le droit au respect de la vie privée et familiale, ni d'aucune disposition constitutionnelle ou légale, que la preuve obtenue en violation d'un droit fondamental ne soit jamais admissible. C'est le juge qui décide quelles sont les conséquences de l'irrégularité. Il dispose donc d'un pouvoir d'appréciation fort large.

La Cour de cassation a considéré dans un arrêt du 27 février 2001 que le droit au respect de la vie privée consacré par l'article 8, alinéa 1er, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, n'est pas un droit absolu et que cette disposition n'empêche pas que, sur la base d'une présomption légitime de l'implication de son employé dans des infractions commises à son détriment, un employeur prenne des mesures afin de prévenir ou de constater de nouveaux faits punissables au moyen de vidéosurveillance dans un espace accessible au public du magasin qu'il exploite.

Suivant la Cour, cette surveillance n'implique pas d'ingérence dans l'exercice du droit au respect de la vie privée au sens de l'article 8, alinéa 2, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, et cette disposition conventionnelle n'exige pas que ladite mesure prise par l'employeur soit préalablement annoncée[2].

---

1. Note précitée du Ministère public à la Cour de Cassation.
2. Note précitée du Ministère public à la Cour de Cassation.

Arrêt de la Cour de cassation du 2 mars 2005

En l'espèce, les éléments de preuve produits contre la demanderesse (employée à la caisse d'un magasin) reposait exclusivement sur une vidéosurveillance dont elle avait fait l'objet sur les lieux de son travail, sans en avoir été informée préalablement.

La demanderesse invoquait donc parmi les moyens en Cassation, la violation de l'article 9 de la convention collective de travail n° 68[1] (obligation d'information du travailleur).

La Cour de Cassation a rejeté ce moyen, en considérant, par application des principes développés infra, que c'est au juge qu'il appartient d'apprécier les conséquences de l'irrégularité dans l'obtention des preuves contre la demanderesse;

En l'espèce, la Cour de Cassation a estimé que c'est à la suite d'une présomption légitime de l'employeur que son employée pourrait avoir commis des infractions, que ce dernier a installé, dans le magasin où elle travaillait, un dispositif de vidéosurveillance. Ce dispositif visait uniquement la caisse sur laquelle la demanderesse enregistrait les achats des clients.

La cour a considéré que le dispositif de vidéosurveillance incriminé était destiné à permettre la constatation d'infractions dont la demanderesse était soupçonnée depuis plusieurs années, que ce dispositif était adéquat et ne portait pas atteinte à sa vie privée ni n'entravait son droit de contredire librement devant les juridictions de jugement les éléments produits à sa charge.

Dans un autre moyen, la demanderesse invoquait également une violation des articles 4, 9 et 17 de la LVP. La Cour de Cassation a également rejeté ce moyen au motif que la caméra de surveillance était fixée uniquement sur la caisse enregistreuse du magasin, dans un lieu accessible au public et non sur la demanderesse elle-même. Par conséquent, les données enregistrées n'avaient pas de caractère personnel au sens de la LVP[2].

---

1. Voir infra 2.2.4.
2. On peut s'interroger sur ce raisonnement puisque l'article 1er de la LVP définit les données à caractère personnel comme « toute information concernant une personne physique identifiée ou identifiable (...) ». Même si la caméra n'était orientée que sur la caisse enregistreuse du magasin, la caissière y travaillant devait vraisemblablement être identifiable ne serait-ce qu'au moyen de la date et des heures où les images étaient enregistrées.

3.1.*2.3. Utilisation de caméras à des fins professionnelles*

3.1.2.3.1. Quelques régimes visant certaines professions

– Les prescriptions V.R.T. stipulent que toute utilisation d'un enregistrement avec une caméra cachée doit être préalablement autorisée par écrit par la personne concernée[1]. Pour la télévision privée et les radios locales, il existe de vagues renvois à la déontologie des journalistes[2].

– Les inspecteurs sociaux peuvent, dans le cadre de leurs compétences, faire des constatations au moyen de photos, d'enregistrements filmés ou vidéo[3].

– Pour les huissiers de justice il existe une circulaire de la Chambre (professionnelle) nationale qui leur interdit de procéder à des filatures, de faire des prises de vue ou de photographier au téléobjectif. Les constatations faites en secret ne sont pas acceptées comme preuve valable [4].

– La loi du 10 avril 1990 sur les entreprises de gardiennage, les entreprises de sécurité et les services internes de gardiennage stipule que personne ne peut être l'objet d'une surveillance ou protection particulière par une entreprise ou un service interne de gardiennage, sans y avoir donné son consentement exprès[5]. Contrairement à la loi sur les détectives (*infra)*, la loi ne contient pas de dispositions qui visent explicitement l'utilisation de techniques visuelles.

  Il n'est actuellement en tout cas pas clair de savoir comment l'utilisation de caméras par les entreprises de gardiennage s'inscrit dans la philosophie de la loi du 10 avril 1990. Cette loi, qui est moins stricte que celle sur les détectives (*infra*), part en effet du principe que les agents de gardiennage sont visibles physiquement et peuvent donc aisément être contrôlés par le citoyen. Toutefois, lorsque des agents de gardiennage observent des images au départ d'une

---

1. Voir article 43 des « Voorschriften, gebruiken en aanbevelingen inzake radio- en tv- berichtgeving voor de journalisten van de B.R.T. » publ. in NEELS, L., VOORHOOF, D. et MARTENS, H., *Media-lex,* Antwerpen, Kluwer rechtswetenschappen, 1990, 505.
2. Voir VOORHOOF, D. et BREWAEYS, E., note sous Bruxelles, 26 octobre 1989, *R.G.D.C.B.*, 1991, n° 3, 248.
3. Loi du 16 novembre 1972 concernant l'inspection du travail, Voir à ce sujet « Bevoegdheden van de sociale inspecties », *Sociale Actualiteit,* 18 avril 1990, n° 302, 3.
4. BERTRAND, J.C., « De vaststelling van overspel », *De Gerechtsdeurwaarder*, 1992, 1, 18.
5. Article 8 § 5 in fine L. 10 avril 1990 sur les entreprises de gardiennage, les entreprises de sécurité et les services internes de gardiennage, *M.B.,* 29 mai 1990.

caméra de contrôle, cette garantie disparaît et il n'y a plus de contrôle direct du citoyen sur les faits et gestes des agents de gardiennage. Par ailleurs, dans ce cas, l'autorisation expresse de la personne surveillée exigée par la loi fait souvent défaut.

– La loi du 30 octobre 1998 insère un article 442bis au Code pénal en vue d'incriminer le harcèlement[1]. La nouvelle disposition stipule ce qui suit: *« Quiconque aura harcelé une personne alors qu'il savait ou aurait dû savoir qu'il affecterait gravement par ce comportement la tranquillité de la personne visée, sera puni d'une peine d'emprisonnement de quinze jours à deux ans et d'une amende de cinquante francs à trois cents francs, ou de l'une de ces peines seulement. Le délit prévu par le présent article ne pourra être poursuivi que sur plainte de la personne qui se prétend harcelée »*. Les travaux préparatoires de la loi montrent que le législateur a hésité entre une appréciation stricte ou large de la notion de 'harcèlement'. A certains endroits il utilise ou suggère en effet une large appréciation de la notion, ce qui signifie concrètement que, par exemple, la filature de personnes ou le fait de l'observer pendant un long moment des personnes avec ou sans caméra tomberait sous le coup de cette disposition[2].

3.1.2.3.2. Utilisation de caméras par des détectives privés

Les détectives accomplissent, tout comme les entreprises de gardiennage d'ailleurs, des missions voisines des tâches de police et c'est la raison pour laquelle ils sont strictement contrôlés en Belgique. Une étude nous apprend que les détectives privés utilisent les méthodes visuelles suivantes en Belgique: lire des lettres, examiner des déchets, regarder à l'intérieur et pénétrer dans une habitation, épier, suivre et effectuer des prises de vues et infiltrer[3].

1. Loi du 30 octobre 1998 qui insère un article 442bis dans le Code pénal en vue d'incriminer le harcèlement, *M.B.*, 17 décembre 1998.
2. Comp. Exposé des motifs de la proposition de loi insérant l'incrimination du harcèlement*, Doc. Parl.*, Chambre, Session ordinaire, 1996-1997, n° 1046/ 1 et aussi le Rapport fait par monsieur Th. Giet, *Doc. Parl.*, Chambre, Session ordinaire, 1996-1997, n° 1046/8.
3. VAN LAETHEM, W., DECORTE, T. et BAS, R., *Private politiezorg en grondrechten,* Leuven, Universitaire Pers, 1995, 125-155.

La loi du 19 juillet 1991

La loi du 19 juillet 1991 organisant la profession de détective privé[1] interdit aux détectives privés de recueillir des informations sur les convictions politiques, religieuses, philosophiques ou syndicales, sur l'état de santé et – sauf exception – sur les penchants sexuels de ses concitoyens[2]. Suite à une modification législative de 1996, on y a ajouté l'appartenance mutualiste et l'origine sociale ou ethnique de tiers[3]. Le législateur a voulu via cette disposition protéger spécialement certains éléments de la vie privée en les excluant de toute investigation[4]. Selon la doctrine, de telles investigations sont punissables même moyennant autorisation de la personne concernée donnée au détective ou au mandant du détective, parce que ces dispositions sont d'ordre public[5].

Le régime initial en matière d'utilisation de caméras

Jusqu'en 1997, la loi du 19 juillet 1991 comportait également une disposition qui imposait aux détectives privés une interdiction « *d'espionner ou de faire espionner ou de prendre ou de faire prendre intentionnellement à l'aide d'un appareil quelconque des vues de personnes qui se trouvent dans des lieux non accessibles au public sans que le gestionnaire du lieu OU les personnes concernées aient donné leur consentement à cette fin* »[6]. Cette disposition, combinée à l'article 19 de la loi, incrimine le fait d'espionner ou de prendre des vues de personnes pour autant que cela se fasse à l'aide de certains appareils, par exemple un téléobjectif, et que soit les personnes en question, soit le gestionnaire du lieu n'aient pas donné leur consentement[7]. La mise en place des appareils dans le but de commettre les infractions précitées est également punissable.

---

1. Loi du 19 juillet 1991 organisant la profession de détective privé, *M.B.*, 2 octobre 1991, err. *M.B.*, 11 février 1993, Loi du 10 avril 1990 sur les entreprises de gardiennage, sur les entreprises de sécurité et sur les services internes de gardiennage, *M.B.*, 29 mai 1990. Voir aussi les rapports annuels sur cette dernière loi édités par la Police générale du Royaume chez Politeia.
2. Voir art. 7 L. 19 juillet 1991 organisant la profession de détective privé, *M.B.*, 2 octobre 1991.
3. Article 7 L. 19 juillet 1991 modifié par l'article 7 L. 30 décembre 1996 modifiant la Loi du 19 juillet 1991 organisant la profession de détective privé, *M.B.*, 14 février 1997. On lira: VOSSEN, B., « Une mise à jour de la loi sur les détectives privés », *Vigiles*, 1997, 1, 42; CAPPELLE, J. et VAN LAETHEM, W., *o.c.*, Bruxelles, Editions Politeia SA., 1997, 197p.
4. CAPPELLE, J. et VAN LAETHEM, W., *o.c.*, 120. Ces auteurs commentent in extenso les interdictions.
5. CAPPELLE, J. et VAN LAETHEM, W., *o.c.*, 120.
6. Voir art. 5 L. 19 juillet 1991 organisant la profession de détective privé, *M.B.*, 2 octobre 1991.
7. Exposé des motifs du projet de loi organisant la profession de détective privé, *Doc. Parl.*, Sénat, 1990-1991, 1259/1, 8.

L'Exposé des motifs de la loi ajoute les éclaircissements suivants: *« Ces actes ne sont toutefois punissables que si les personnes en cause se trouvent dans des lieux non accessibles au public, tel qu'un logement privé. En ce sens, l'espionnage et la photographie de quelqu'un qui se trouve sur la voie publique ne sont pas punissables dans le cadre de la présente loi. Cela ne porte bien entendu pas préjudice à la jurisprudence existante sur le plan civil en matière de reproduction de photos »*[1]. Dans la doctrine, la notion de 'lieu non accessible au public' a été considérablement clarifiée sur la base des exemples tirés d'autres législations et des dispositions constitutionnelles relatives à la liberté de réunion[2]. Cette situation se produit généralement lorsque l'accès est fermé ou lorsque des titres d'accès individualisés sont exigés et qu'ils sont contrôlés. Concrètement, cela signifie que seuls les lieux privés, comme une habitation privée, l'espace fermé d'une entreprise ou le lieu où se déroule une fête privée tombent sous le coup de la protection pénale. L'observation ou la réalisation de prises de vues dans des lieux accessibles au public (comme par ex. des magasins, des cafés ou des dancings) et dans des lieux publics (parcs, rues) n'est pas punissable, sous réserve de la protection légale accordée par le droit d'auteur et les droits fondamentaux[3].

Les nouvelles règles plus strictes applicables à l'utilisation de caméras

La loi du 30 décembre 1996 modifiant la loi sur les détectives réécrit l'article 5 de la loi sur les détectives dont un des aspects était jugé trop large. La simple autorisation du gestionnaire d'un lieu ne suffit plus pour pouvoir, en secret, filmer ou réaliser des vues de toutes les personnes présentes. L'alinéa premier nouveau de l'article 5 de la loi dit désormais: *« Il est interdit au détective privé d'espionner ou de faire espionner ou de prendre ou de faire prendre intentionnellement des vues de personnes qui se trouvent dans des lieux non accessibles au public, à l'aide d'un appareil quelconque, sans que le gestionnaire du lieu ET les personnes concernées aient donné leur consentement à cette fin »*[4].

Désormais, la prise de vues n'est plus seulement soumise à l'autorisation préalable du gestionnaire du lieu mais aussi à celle des personnes qui s'y trouvent. Cette dou-

1. Idem.
2. CAPPELLE, J. et VAN LAETHEM, W., o.c., 114, avec renvoi à LANCKSWEERDT, E., « Het toepassingsgebied van de Wet van 10 april 1990 op de bewakingsondernemingen, de beveiligingsondernemingen en de interne bewakingsdiensten », in *Bewaking en beveiliging*, Brugge, Die Keure, 1991.
3. CAPPELLE, J. et VAN LAETHEM, W., *o.c.*, 114-115.
4. Article 5 modifié par l'article 5 L. 30 décembre 1996 modifiant la Loi du 19 juillet 1991 organisant la profession de détective privé*, M.B.,* 14 février 1997.

ble exigence d'autorisation[1] s'inscrit dans la ligne de la philosophie de base de la stricte interdiction d'écoute prévue par la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées (infra).
La double autorisation doit être donnée au préalable. La réalisation de photos est illégale si les personnes intéressées donnent leur accord a posteriori[2]. D'après la doctrine, l'autorisation peut ressortir des circonstances ou être donnée explicitement (oralement ou par écrit)[3].

L'article 1er, § 2 de la loi du 19 juillet 1991 stipule explicitement que les journalistes, les huissiers de justice, les notaires, les avocats et les généalogistes n'entrent pas dans son champ d'application[4]. L'interdiction de collecter certaines informations sensibles et celle de faire des prises de vues et d'espionner des personnes, ne vaut donc que pour les détectives privés et pas pour les autres citoyens. Le Conseil d'Etat a notamment souligné que cette situation est peu satisfaisante. Tout le monde peut en effet utiliser des appareils d'observation ou récolter des informations sur des personnes. Le contenu de ces garanties devrait, en d'autres termes, s'appliquer à tous les citoyens et pas seulement aux détectives privés [5].

Que peut-on faire en présence de détectives qui observent ou qui filment?

Pour contrôler si le détective privé est resté dans les limites légales, la loi sur les détectives privés prévoit deux moyens. En premier lieu, la personne qui se sait filmée ou filée est libre de s'adresser au juge civil. Celui-ci peut contraindre le détective privé à lui remettre la convention, dont question à l'article 8 de la loi sur les détectives, et le rapport destiné à son client, dont question à l'article 9 de la loi sur les détectives, afin de pouvoir se faire une idée des actes posés par le détective privé à la lumière des lois existantes.

En deuxième lieu, la loi prévoit des compétences de contrôle et des possibilités de sanction dans le chef des fonctionnaires de la Police générale du Royaume. Ce service fait partie du ministère de l'Intérieur. Sur la base de l'article 17 de la loi, ces

1. CAPPELLE, J. et VAN LAETHEM, W., *o.c.,* 115.
2. CAPPELLE, J. et VAN LAETHEM, W., *o.c.,* 116.
3. CAPPELLE, J. et VAN LAETHEM, W., *o.c.,* 116.
4. D'autres professions ne sont pas exclues par la loi mais par arrêté royal. C'est ainsi que l'arrêté royal du 30 juillet 1994 exclut notamment les assistants sociaux et les experts judiciaires. Cf. A.R. 30 juillet 1994, *M.B.*, 14 septembre 1994.
5. Conseil d'Etat, avis sur le projet de loi organisant la profession de détective privé, *Doc. Parl.,* Sénat, 1990-1991, n° 1259/1, 38.

fonctionnaires disposent du droit de dresser des procès-verbaux qui ont force probante jusqu'à preuve du contraire. Ils disposent également de larges compétences de recherche. C'est ainsi qu'ils peuvent notamment avoir accès à l'agence du détective privé pendant les heures habituelles d'ouverture ou de travail et qu'ils peuvent procéder à toute enquête, tout contrôle et toute audition, prendre tous les renseignements qu'ils estiment nécessaires afin de s'assurer que les dispositions de cette loi et de ses arrêtés d'exécution sont respectées, et en particulier se faire produire sur place les documents, pièces, registres, livres, disques, bandes magnétiques ou supports informatiques, qu'ils estiment nécessaires dans le cadre de leurs recherches et de leurs constatations et en prendre des extraits, des copies ou des doubles. Cette voie est sans aucun doute la plus adaptée et la moins onéreuse.

Il n'est pas clairement établi si la Commission de la protection de la vie privée est compétente en la matière. Malgré sa dénomination, la Commission n'est pas compétente pour tous les problèmes qui touchent à la vie privée. Plus précisément, la loi du 8 décembre 1992 sur la protection de la vie privée exige qu'il soit question d'un traitement de données personnelles, ce qui implique que le détective privé soit stocke les informations qu'il aura trouvées dans un ordinateur, soit qu'il les intègre dans un fichier manuel structuré. Si le détective privé fait des photos avec un appareil photo digital, cette condition semble être remplie. Il n'en va pas de même si le détective se limite à filer une personne et à prendre des notes à ce sujet.

La loi du 19 juillet 1991 ne dit nulle part comment le détective privé doit établir la convention et le rapport pour le client. Dans la littérature spécialisée, on insiste en outre pour que les intéressés n'établissent *pas* les deux documents en question de façon automatisée, afin d'exclure toute falsification au niveau du contenu. On ne peut donc pas dire avec certitude que la loi du 8 décembre 1992 est applicable, que la Commission peut intervenir dans ce cadre et que l'on peut s'adresser directement au détective privé en question pour lui demander la communication de ses données personnelles sur la base de la loi précitée.

Quelle que soit la voie empruntée, reste un autre problème, en l'occurrence celui de savoir si le détective privé en question a agi ou non de façon légitime. Ce problème nous semble être le plus pertinent. Outre les dispositions déjà commentées de la loi sur les détectives, qui sont généralement comprises comme des limites de compétence négatives, la loi ne détermine pas ce que peut ou ne peut pas faire un détective. Le point de départ semble être « *Ce qui n'est pas interdit est autorisé* ». Il est, par conséquent, loin d'être clair de savoir si un citoyen peut agir contre un détective qui filme sur la voie publique, par exemple. Pour savoir ce qui est permis et ce qui ne l'est pas, le justiciable doit donc se contenter de la maigre jurisprudence et des

rares exemples de ce que peuvent réellement faire les détectives privés cités dans les travaux préparatoires de la loi sur les détectives. Les travaux parlementaires de la loi sur le harcèlement contiennent également des informations (confuses).

Les pages 109 jusqu'à 154 ont été suprimées.