

Projet S.T.S. Informatique 4^{ème} année

"Big Brother" ou nécessité, quelle est la finalité de la surveillance vidéo?

Ses dérives et les moyens de s'en protéger

Edouard Forler et Rafael Herrera
juin 1999

Introduction

Dans les rues, les jardins publics, les gares, les aéroports, les magasins, les galeries commerciales, les musées, les banques et les parkings, les caméras ont proliféré de manière considérable. Tous ceux qui aujourd'hui parcourent ces lieux sont susceptibles de pénétrer dans le champ de vision de caméras de surveillance et désormais les moindres faits et gestes peuvent être observés à distance sur un écran.

Les premiers systèmes de vidéosurveillance ont été installés au début des années 70 pour apporter une aide à la régulation du trafic routier et pour lutter contre les vols dans les banques et les commerces de luxe. Tout au long des années 80, ces systèmes se sont multipliés dans les transports collectifs, les commerces, les lieux de travail et de loisirs et aux abords des bâtiments publics. Un pas de plus vers la banalisation a été franchi, au début des années 90, quand des caméras ont été installées sur la voie publique, dans les stades et dans les rues de certaines villes.

La prolifération de ces équipements semble répondre à un impératif sécuritaire provoqué par la montée de délinquances et d'incivilités dans l'espace urbain. Mais la prévention des atteintes à la sécurité des personnes et des biens suffit-elle à justifier le recours à de tels procédés?

A travers la présentation des principales techniques développées ces dernières années, ainsi que des buts de la vidéosurveillance, nous nous proposons de mettre en évidence le caractère dangereux sur le plan éthique de ce procédé, s'il n'est pas correctement maîtrisé.

Nous verrons notamment que l'évolution rapide des technologies empêche souvent la loi d'être suffisamment efficace pour se protéger contre les dérives; nous espérons également susciter chez le lecteur l'envie de s'interroger sur les conséquences de la présence d'une mention aussi anodine que "Souriez, vous êtes filmé" lorsqu'il se rendra dans son supermarché habituel.

Sources

Notre recherche a débuté sur le World Wide Web, où nous avons été surpris de trouver plus d'informations que prévu, surtout sur les sites français. En fait, la France semble particulièrement préoccupée par le problème: plusieurs émissions télévisées ont été consacrées au sujet; celles-ci nous ont d'ailleurs permis d'élaborer la base de notre discussion. Le World Wide Web nous a également permis de trouver quelques livres et articles traitant de ce sujet.

Nous tenons à remercier M. Emmanuel Bloch, de la Faculté de Droit de l'Université de Lausanne, qui nous a facilité l'accès aux données juridiques, plus particulièrement en ce qui concerne l'atteinte à la vie privée et l'administration des preuves illicites en Suisse.

Etat de l'art

Les dispositifs actuels sont de plus en plus performants: certaines caméras peuvent surveiller un champ de vision sur 360 degrés; d'autres sont munies de zooms capables de lire les prix frappés par une employée de caisse ou une plaque minéralogique à 300 mètres; certaines, dites intelligentes, comportent des détecteurs qui donnent l'alerte en cas d'incident. La transmission des images par les réseaux téléphoniques grand public peut permettre de voir et d'écouter sans frontière, à l'échelle de la planète.

Plusieurs organismes de standardisation internationaux travaillent sur des normes de transmissions et de compression capables d'exploiter les moyens de télécommunications actuelles, tel que Internet et la téléphonie mobile, tout en restant compatibles avec les standards vidéos déjà existants, comme l'est la norme MPEG2 utilisée dans la télévision digitale.

Les recherches actuelles s'orientent dans les domaines de la compression et de la cryptographie. Les premières techniques permettent d'augmenter le débit vidéo tout en gardant une certaine qualité d'image, tandis que les deuxièmes essaient de maintenir l'intégrité des données envoyées par les caméras, pour éviter les falsifications et les trucages.

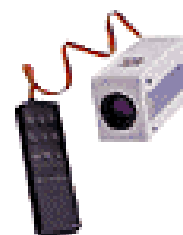
La recherche militaire est aussi à la pointe du développement avec les caméras infrarouges pour la vision nocturne et les caméras thermiques permettant de détecter des êtres à sang chaud à travers les murs. Mais, tout ces équipements sont coûteux et ne sont pas accessibles au commun des mortels. De plus leur utilisation diverge du sujet que nous sommes en train de traiter.

La mise au point de logiciels de surveillance permet une observation en quelque sorte "objective", centrée sur le repérage d'une anomalie de comportement, d'une tenue vestimentaire atypique ou d'une origine ethnique particulière. A la différence d'un opérateur humain, la machine de vision effectue un enregistrement automatique dans le champ dans lequel elle opère. Mais attention, les fausses interprétations peuvent avoir des conséquences redoutables!

Voici quelques exemples de systèmes de vidéo surveillance. Cette liste ne se veut pas exhaustive, mais elle donne une bonne idée des différentes techniques utilisées.

Systèmes classiques:

- Voici une caméra qui permet de faire un zoom avec la commande à distance pour vérifier quelque chose en détail. Idéale pour surveiller les entrées, cette caméra combinée est une solution rentable pour les installations qui demandent une commande de zoom. 410 lignes, 2 lux, compensation de contre jour, balance automatique de blanc, obturateur électronique à grande vitesse et diaphragme automatique sont les caractéristiques disponibles pour une utilisation dans une très large plage de luminosité à l'intérieur comme à l'extérieur.
- Cette autre caméra mesure seulement 25 mm de diamètre et 56 mm de longueur. Elle est idéale pour une surveillance discrète à l'extérieur. Ces



caractéristiques sont les suivantes : 380 lignes de résolution, 0,1 lux, objectif grand angle de 3,6mm.

- Idéal pour la surveillance dans plusieurs directions à partir d'un élément discret installé au plafond, il est possible d'avoir un dispositif composé de 1, 2 3 ou 4 caméras avec 400 lignes de résolution, 0,1 lux et une taille de 17,2 cm de côté x 6,4 cm d'épaisseur.



Systemes dissimulés:

- Les miroirs "pour regarder dans les coins" sont une banalité dans la plupart des magasins, mais si ceux-ci ont une caméra vidéo invisible à l'intérieur, alors on pourra surveiller ce qui se passe, alors que les personnes pensent que l'on ne regarde pas.



- Il existe aussi des systèmes vidéo ressemblant à une lampe d'éclairage ou un détecteur de mouvements, mais qui en réalité contiennent une caméra vidéo. La particularité de cette caméra vidéo est qu'elle comprend un objectif grand angle qui peut être ajusté vers le bas et / ou sur le côté.



- Cette caméra est dissimulée dans une véritable horloge avec mouvements des secondes. L'objectif est complètement invisible derrière la face avant opaque de l'horloge et ne peut être vu tant que celle-ci est fermée. La caméra est montée sur cardan ce qui permet un angle de vue réglable.



- Voici une caméra vidéo dans un détecteur de fumée, virtuellement impossible de le différencier d'un vrai car le système est construit à l'intérieur d'un vrai détecteur de fumée. On peut y installer jusqu'à 5 caméras de façon à avoir une vision sur 360°.



- Une caméra dissimulée dans un haut-parleur de plafond fonctionnel est une des caméras les moins détectables qui soient. Si en plus on raccorde le haut-parleur avec de la musique d'ambiance ou un système d'appel, personne ne pourra suspecter que c'est une caméra.



- Une caméra placée dans un réel panneau lumineux "Exit", exigé dans beaucoup d'endroits, est très bien comme système de surveillance invisible. Ce système est idéal pour le contrôle d'entrées.



- Il existe aussi des caméras noir et blanc dissimulées dans des encadrements réels de photo en chêne.



- Une caméra vidéo peut aussi être dissimulée dans une lampe encastrée moderne.



En Angleterre et aux Etats-Unis, les caméras dites "intelligentes" permettent déjà de repérer les véhicules en excès de vitesse sur les autoroutes, et de retrouver, par réseau informatique interposé, le numéro de carte grise du véhicule et le nom de son propriétaire [1]. Ces caméras sont donc équipées d'un équipement de mesure de la vitesse, de systèmes de vision de nuit, de reconnaissance de forme, d'identification de la plaque minéralogique et d'une connexion en réseau informatique! On frémit en pensant à la banalisation de tels systèmes.

Les formes de la vidéosurveillance

Nous pouvons distinguer deux formes différentes de vidéosurveillance: une, dite de prévention, entend établir une relation qui incite la personne à adopter le comportement requis; l'autre dite de répression, se contente d'intervenir en cas de comportement indésirable.

La prévention

Pendant plus de trois siècles, c'est par la maîtrise de soi et l'autodiscipline qu'a pu être obtenue la pacification des mœurs et des comportements. La formation d'une société de cour, aux XVII^{ème} et XVIII^{ème} siècles, a éliminé les affrontements violents et contribué à étendre à l'ensemble de la société de nouvelles normes de comportements à base de contrôle de soi.

Ce sont les systèmes disciplinaires qui ont fabriqué, à partir de la fin du XVIII^{ème} siècle, l'individu approprié. Ce dernier a été rendu docile et utile grâce à l'enfermement dans des lieux clos (école, caserne, usine, hôpital, prison). Enfermé, l'individu surveillé reprend à son compte les contraintes du pouvoir.

Depuis les années 50, la modernité a donné lieu à des endroits, comme les aéroports ou les grands centres commerciaux, où ne s'expriment que des identités partielles et anonymes. C'est dans ce contexte que la vidéo tente de moderniser les dispositifs de surveillance. La fonction générale d'être vu sans jamais voir, jusqu'alors réservée à des espaces fermés, va être appliquée aux espaces ouverts fréquentés par des individus de plus en plus mobiles.

Quand on se sent surveillé par des caméras, même s'il n'y a personne à la régie, on est conditionné, et il y a une sorte de commandement. La vidéosurveillance est un commandement des comportements. En même temps qu'elle dissuade les délinquants, elle modifie les comportements de tout le monde.

Selon l'American Management Association, 35% des sociétés américaines surveillent les appels téléphoniques, les messageries vocales et les fichiers personnels, et 34% utilisent la vidéosurveillance.

L'important est que le vidéosurveillé sache qu'il fait l'objet d'une surveillance. C'est cette connaissance qui établit la relation disciplinaire et amène l'individu à adopter la conduite qu'on attend de lui. L'efficacité du schéma de surveillance provient de la relation «être vu sans jamais voir». C'est pourquoi cette forme de technosécurité est très apparente et annoncée très explicitement à l'aide d'une information du type: «Souriez, vous êtes filmé.»

Certaines formules permettent parfois de faire jouer à l'individu le double rôle de surveillé et de surveillant. Par exemple, des systèmes actuellement expérimentés dans des immeubles collectifs donnent la possibilité à tout habitant de suivre, sur son téléviseur, les allées et venues des personnes se trouvant dans les parties communes.

La répression

La finalité de la vidéosurveillance est de nature à lui donner une forte légitimité. La sécurité est en effet un des premiers droits humains. Or le nombre d'agressions contre les biens et les personnes s'est accru en Europe, même si les meurtres restent rares. En France, par exemple, entre 1963 et 1991, les vols avec violence ont été multipliés par 23, et les cambriolages par 8. Alors que la police parvenait à résoudre la moitié des affaires de vol en 1950, le chiffre n'était plus que de 12,5 % en 1993.

C'est pourquoi, dans les années 70, est apparue une demande de sécurité de proximité, à laquelle la police traditionnelle ne semblait pas pouvoir répondre. La solution a été recherchée ailleurs, dans le recours à des services privés ou municipaux de sécurité et dans des technologies comme la vidéosurveillance.

Les chiffres montrent que celle-ci améliore parfois la sécurité. Ainsi en France, dans les banques (90 % des agences sont équipées de caméras), 50 % des voleurs sont désormais identifiés et arrêtés dans les deux ans qui suivent l'agression ; dans le métro parisien, 83 % des incidents sont détectés grâce à la vidéo, et le nombre des interpellations a augmenté de 36 %; les responsables de grands magasins constatent également que, grâce à cette technique, le chapardage a chuté des deux tiers.

Parfois, cependant, la technosécurité ne fait que déplacer la délinquance, les malfaiteurs poursuivant leur activité là où il n'y a pas de caméras. Ainsi, le taux moyen de criminalité à Monaco, ville quadrillée par plus de 60 caméras munies de zoom, n'est que de 44 crimes et délits pour 1000 habitants, mais ce chiffre est monté à 130 pour 1000 dans le département voisin des Alpes-Maritimes (la moyenne française étant de 90 pour 1000).

L'implantation de caméras n'apporte pas toujours l'efficacité attendue. Parmi les villes les plus équipées de France, Levallois-Perret, dans la banlieue parisienne, dont les rues sont gardées par 86 caméras, a connu, en 1996, une progression de la délinquance, avec une forte hausse des vols.

Cette seconde forme de vidéosurveillance introduit un nouveau type de contrôle. A travers un mécanisme abstrait, distant, dépersonnalisé, automatique, bureaucratique, et en grande partie invisible et incompréhensible, la machine crée des informations et peut également provoquer des actions.

Le contrôle se symbolise plutôt par la manipulation que par la coercition, par des ficelles invisibles maniées de loin. Le sujet surveillé est réduit à n'être qu'un objet d'information. Après les nombreux fichiers constitués sur lui et les traces électroniques qu'il laisse, les caméras vidéo viennent enrichir la transparence de l'individu, par un suivi à partir de son image. La personne surveillée reste ignorante des procédures et des manipulations qui s'effectuent derrière son dos.

Malheureusement, la multiplication de ces systèmes va de paire avec la multiplication des problèmes de droit élémentaire. Une liberté essentielle comme celle d'aller et venir librement dans un espace public sans être observé, est régulièrement foulée au pied: un juge administratif français, en 1990, a annulé la délibération du conseil municipal d'une ville approuvant la création d'un système de vidéosurveillance. Le juge a estimé que l'installation généralisée et le fonctionnement permanent de caméras portaient une atteinte excessive aux libertés individuelles, et notamment au droit à la vie privée et à l'image, qui n'était justifiée ni par une

habilitation judiciaire, ni par les nécessités de l'ordre public ou la constatation ponctuelle d'infractions au code de la route ou d'atteinte aux biens ou aux personnes.

Les dérives

Bien des dérives sont envisageables avec l'usage des systèmes de vidéosurveillance, ainsi qu'avec d'autres technologies (transactions plus ou moins sécurisées pour le commerce sur l'internet par exemple). Il convient toutefois d'examiner dans quelle mesure ces dérives sont réelles.

Des menaces sont souvent évoquées au sujet des systèmes de surveillance concernant les libertés individuelles; En particulier, l'usage de ces systèmes par des organismes étatiques, que ce soit dans des sociétés démocratiques ou non, afin de contrôler la population, a fait l'objet de nombreuses oeuvres littéraires et cinématographiques. La plus connue de ces oeuvres est sans doute "1984", de Georges Orwell [9], qui décrit un monde dans lequel toutes les libertés ont été anihilées par le contrôle des esprits. Ce contrôle est notamment exercé par l'usage d'appareils appelés "télécrans", qui, tout en informant les citoyens, permettent également de les surveiller étroitement, y compris dans leur vie privée.

Cette vision, quelque peu exagérée, d'un monde totalitaire, évoque les dérives politiques de la télé-surveillance et de la vidéosurveillance. Nous n'avons pas découvert dans notre recherche de telles dérives directes de manipulation de la population, et il faut bien reconnaître qu'avec la puissance actuelle des médias dans les pays réellement démocratiques, il serait très difficile de maintenir et d'exploiter une telle situation de "complot global".

On mentionnera tout de même l'usage des caméras qui a été fait sur la place Tiananmen à Pékin en juin 1989, qui montre que l'absence de démocratie et la vidéosurveillance peuvent faire bon ménage: en effet, suite aux événements survenus à cette époque, les autorités ont soigneusement décortiqué les bandes vidéos prises sur la place afin d'identifier et de réprimer plusieurs des manifestants, jugés responsables des émeutes. On ne s'attardera pas sur l'effet de crainte induite sur la population, qui représente une forme de contrôle de l'esprit.

Il existe en réalité d'autres dérives bien plus insidieuses. En Europe et aux Etats-Unis, les systèmes de vidéosurveillance se sont multipliés durant ces dix dernières années: Rien qu'en France, le chiffre d'affaires de la vidéosurveillance a augmenté de 51% de 1991 à 1996 [7], alors que ce pays est l'un des plus avancés en ce qui concerne la régulation de son usage. L'argument majoritaire déployé par les consommateurs de cet instrument est bien sûr la prévention des crimes et de la délinquance, pour laquelle le système est souvent présenté comme l'arme ultime.

Cependant, compte tenu de l'absence de principes d'utilisation strictes, les dérives liberticides se sont multipliées, afin de mieux servir les intérêts de quelques initiés; Alors que l'on clame haut et fort que la mise en place de caméras permet de protéger le citoyen et d'éviter les agressions et les crimes, on se rend compte qu'en réalité, outre l'usage répressif (on ne compte plus les affaires de hooliganisme dans lesquelles des personnes coupables d'agression caractérisée ont été confondues par l'oeil intransigeant de la caméra), il existe un usage à but véritablement lucratif du système.

Lucratif au sens direct du terme? Parfois. Comme lors de ce cas de diffusion des images prises par les caméras d'un hypermarché dans le rayon textile: celles-ci avaient été installées dans le but de réduire les vols de vêtements par la surveillance discrète des cabines d'essayage. Un employé y a trouvé le moyen de se faire un peu d'argent de poche en exploitant le côté voyeur de la chose. Un exemple similaire s'est produit avec la surveillance d'un parking de nuit [12].

Lucratif au sens indirect du terme, sûrement. L'atteinte à la vie privée et à l'image est parfois reconnue nécessaire, par exemple lorsqu'il s'agit de démasquer les employés indéliçables, que ce soit pour des cas de vol ou de dégradation, mais aussi dans le cas où ils ne seraient pas assez productifs pour l'entreprise. C'est précisément ce qu'il s'est produit dans l'affaire Richardson contre Davis Wire Industries, Ltd. (Canada, avril 1997): un contremaître avait été congédié parce qu'il avait dormi au travail et l'avait subséquemment nié [2]. Plutôt que de confronter la personne fautive directement, son employeur a préféré faire installer une caméra cachée dans le réfectoire de l'entreprise. Ce cas pose d'ailleurs le problème des preuves vidéo obtenues de manière frauduleuse, sur lequel nous reviendrons dans le chapitre suivant. L'employé a été bien évidemment débouté de son recours pour atteinte à la vie privée.

De même, les caméras installées dans les commerces afin de prévenir les vols, sont souvent utilisées pour surveiller le personnel. Présenté comme préventif, l'instrument devient un outil de contrôle de la productivité et est systématiquement présenté comme témoin à charge dans le cas d'un litige entre employé et employeur.

Lucratif au sens indirect toujours, lorsque la caméra est utilisée pour analyser consciencieusement le comportement du consommateur. L'analyse des moindres faits et gestes permet de perfectionner le positionnement des produits et d'induire le parcours d'achat le plus efficace... En France, de véritables supermarchés expérimentaux ont été ainsi construits, dans lesquels les habitudes des clients sont soigneusement décortiquées, de manière scientifique [13]. On étudie l'influence de certaines modifications dans l'organisation ou l'ambiance des rayons sur l'envie d'acheter.

Lucratif enfin, lorsque les bandes vidéos servent (entre autres sources) à alimenter les données statistiques, qui vont permettre d'anticiper la demande des consommateurs dans tel ou tel domaine, et parfois de créer de la demande et des marchés de manière artificielle [12][13].

Des dérives, il y en a aussi sur la voie publique. Elle ne sont pas d'ordre commercial et ne sont d'ailleurs pas clairement établies; Il s'agit surtout de problèmes qui ont été mis en évidence. La surveillance de la circulation, dans la plupart des grandes villes modernes, aide, certes, à réguler le trafic, à rendre les transports en commun plus sûrs, à envoyer des secours dans les délais les plus brefs en cas d'accident... Mais on distingue clairement les ceintures de sécurité (une telle exploitation a été faite par la police en Espagne)... et les gens dans les rues [6][12]. Il a même été démontré à Levallois-Perret, l'une des villes les plus vidéosurveillées de France, qu'il était possible de suivre le trajet d'un automobiliste ou d'un passant, par la simple commutation des prises de vue d'une centaine de caméras judicieusement placées (personne n'en douterait) à travers la ville. Dans le même ordre d'idée, la technique aidant, il est maintenant possible d'espionner les gens dans leur propre

maison, de nuit comme de jour (zooms puissants, amplificateurs infra-rouge). A charge des exploitants de faire respecter les lois en la matière quand elles existent.

Dans un domaine plus léger, on peut citer cette proposition tout à fait récente faite par un conseiller municipal de Bloomsburg en Pennsylvanie, de traquer et de condamner les propriétaires de chiens ne nettoyant pas les déjections sur la voie publique de leur petit compagnon, preuve vidéo à l'appui [14]!

Dans le domaine judiciaire, l'enregistrement des individus auteurs de vols peut toujours alimenter, sous forme de photos, un fichier de suspects ou de récidivistes. La mise au point de systèmes de reconnaissance de criminels en fuite sur des séquences vidéos urbaines peut transformer chacun d'entre nous en terroriste potentiel.

Des dérives, il en existe bien d'autres: des parents filmant à son insu leur baby-sitter, découvrant ses petites manies téléphoniques ou télévisuelles (toutefois cet emploi de la vidéosurveillance a montré son efficacité dans plusieurs affaires de violence sur enfant en bas-âge: dans l'état américain du New Jersey, une loi autorise maintenant un tel usage [26]); un collège technique en Belgique dans lequel on traque le fumeur jusque dans les toilettes, en y disposant des caméras destinées à mieux le confondre; et même jusqu'aux systèmes expérimentés dans les immeubles collectifs, qui donnent la possibilité à tout habitant de suivre, sur son téléviseur, les allées et venues des personnes se trouvant dans les parties communes.

Face à ces problèmes, le citoyen et la justice sont mal armés. La personne surveillée reste encore trop souvent ignorante des procédures et des manipulations qui s'effectuent derrière son dos. Le souci sécuritaire fait peu de cas de la liberté d'aller et venir dans un espace public sans être observé. Même dans les pays avancé en la matière sur le plan juridique, certaines règles sont difficilement applicables et vérifiables.

Bien souvent, l'argument de la sécurité aidant, on oublie que l'atteinte aux libertés individuelles que constituent les prises d'images doit être proportionnelle au but poursuivi; Si les atteintes sont inévitables dans certains lieux d'insécurité, elle ne se justifient pas dans tous les cas. Comment garantir le respect des libertés de l'individu vidéosurveillé?

Les lois et l'éthique

Face à la montée en puissance des systèmes de vidéosurveillance, dont la finalité est de nature à leur donner une forte légitimité, il convient de contrôler l'usage qui en est fait. Par ailleurs, s'il est question de forte légitimité, il s'agit d'examiner dans quel contexte. En effet, cette légitimité provient du fait que, très souvent, on considère l'oeil de la caméra comme un témoin irréprochable et les bandes vidéo comme des preuves éclatantes, voire infalsifiables. Comme nous le verrons plus loin, la justice n'est pas toujours d'un avis aussi catégorique.

Prévention: loi ou simple éthique?

En ce qui concerne le contrôle de l'installation des systèmes de vidéosurveillance, les lois en vigueur sont très souvent inadaptées, voire inexistantes. Les installations sont réalisées en général par des sociétés privées, pour des intérêts privés. Dès lors l'Etat s'en remet au bon sens de chacune des parties et compte sur l'existence d'une éthique intrinsèque (Cela doit aller "de soi") [6][7].

C'est ce qu'il se passe effectivement en Suisse ou aux Etats-Unis; En Suisse, aucune loi n'existe au niveau fédéral pour réguler l'installation des systèmes. Quelques jurisprudences existent au niveau cantonal, plutôt contradictoires [25]. Celles-ci sont d'ailleurs très récentes (après 1995) en comparaison de ce qui se fait dans d'autres pays d'Europe. Aux Etats-Unis, chaque état possède évidemment sa propre législation en la matière, mais la plupart du temps, la liberté est laissée aux exploitants d'utiliser leurs systèmes comme ils le souhaitent.

La France, par contre, s'est interrogée et s'interroge depuis près de quinze ans sur les dérives liées à la vidéosurveillance. Jusqu'à présent, les sociétés de télésurveillance et de gardiennage françaises ne devaient pas fournir de preuves de leur compétences. Cette situation est en train de changer avec le projet Chevènement qui va permettre de transformer "le charlatanisme en professionnalisme" en exigeant notamment une formation approfondie des employés [7].

D'autre part, la France a été un des premiers pays à créer une législation adaptée à l'exploitation des caméras de vidéosurveillance. L'installation de ces systèmes est soumise à des lois sévères. Il est par exemple illégal de vidéosurveiller l'intérieur des immeubles d'habitation ainsi que leurs entrées (loi du 21 janvier 1995) [5, voir aussi en annexe].

Bien que la loi Pasqua encourage la mise en place de la vidéosurveillance dans certains lieux comme les magasins de commerce de détail d'une surface de plus de 6000 m², ou les parcs de stationnement ouverts au public de 200 places et plus, il est bien spécifié qu'à la demande du préfet, "les exploitants des locaux concernés (...) sont tenus de faire connaître les dispositions qu'ils ont arrêté pour assurer le gardiennage ou la surveillance desdits locaux. (...) Le préfet peut vérifier sur place la réalité de ces dispositions." [5][6].

Concernant les systèmes installés sur la voie publique, la législation est encore plus sévère: l'installation de tels systèmes doit concerner des lieux "particulièrement exposés à des risques d'agression ou de vol". Elle est subordonnée à une autorisation délivrée par le préfet, après avis d'une commission départementale présidée par un magistrat. Une information "claire et permanente" doit être donnée au public de l'existence des systèmes [5].

On constate donc que, si dans certains pays, l'Etat fait confiance aux sociétés de surveillance pour appliquer une certaine éthique, l'apparition de dérives a tout de même nécessité de s'interroger sur ce problème.

Repression: le problème de l'atteinte à la vie privée

Dès qu'on parle de vidéosurveillance, il se pose la question de la sauvegarde des libertés individuelles et en particulier de la sauvegarde de la sphère privée. Cet argument est souvent utilisé par la défense pour empêcher la recevabilité de preuves vidéo compromettantes. En l'absence de lois spécifiques, comme c'est le cas dans la majorité des pays, dont la Suisse, on se rabat généralement sur la législation concernant la protection de la personne et la violation de la vie privée.

En Suisse, ces problèmes relèvent de l'article 28 du code civil, selon lequel une atteinte est illicite, à moins qu'elle ne soit justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi. En ce sens, il n'est fait aucune différence entre l'utilisation de caméras vidéo et celle de procédés d'écoute téléphonique par exemple. Une personne filmée à son insu peut donc théoriquement se retourner contre les responsables d'un système de vidéosurveillance pour ce motif.

En France, les litiges dus à la vidéosurveillance relèvent aussi de la législation sur la violation de la vie privée. Toutefois, des lois spécifiques préventives existant concernant l'installation et l'utilisation des systèmes de vidéosurveillance, l'abus de données fournies par le moyen de la caméra fait en plus l'objet de poursuites particulières qui peuvent aller jusqu'à trois ans d'emprisonnement ferme et 300 000 FF d'amende [5]. Il n'est pas difficile en tant qu'exploitant de se retrouver en infraction: il suffit d'avoir conservé pendant plus d'un mois des bandes vidéos sans motif valable (un motif valable serait une enquête policière par exemple), ou d'avoir refusé l'accès à une personne aux enregistrements qui la concerne. Des abus plus importants peuvent avoir des conséquences redoutables. Une partie de ces mesures ont d'ailleurs été étendues aux pays de la communauté européenne dès 1987 (Recommandation R(87)15 sur la protection des données à caractère personnel) [3].

Très souvent, l'atteinte à la vie privée n'est pas manifeste, et est lié à une utilisation efficace de la vidéosurveillance. En cas de litige, le juge doit alors pouvoir faire la part des choses et estimer si l'intérêt prépondérant dont se prévalait l'exploitant du système est justifié. Dans une telle situation, le requérant peut être tout simplement débouté de sa demande. Un cas intéressant dans ce sens s'est produit en Suisse, où une association d'ouvriers, suite au mécontentement de l'un des employés, a porté plainte contre la direction de l'usine après l'installation d'un système de surveillance envahissant. Le tribunal cantonal a jugé qu'étant donné l'intérêt du

système et le fait qu'il se trouvait sur le lieu de travail, il ne pouvait être question de violation de la vie privée des ouvriers. Ce cas est d'autant plus étonnant que la direction s'est ensuite retournée contre l'association pour procédure illégale, en avançant que ladite association ne pouvait porter plainte à la place de l'employé, et... a gagné [15].

Ainsi, en l'absence de loi spécifique, on voit bien que la législation sur la violation de la vie privée n'est pas toujours suffisante pour combattre d'éventuels abus de la vidéosurveillance.

Recevabilité des preuves obtenues par vidéosurveillance

Il ne fait nul doute pour la plupart des cours de justice que la vidéosurveillance est d'une utilité indéniable: ce type de preuves peut être utilisé dans des situations où il est difficile d'établir la vérité. De plus, les films vidéo se substituent parfois aux techniques conventionnelles d'identification d'un coupable parmi plusieurs suspects: on prépare plusieurs séquences d'une scène décrite par le témoin avec les différents suspects en guise de premier rôle.

Les preuves vidéo, très utiles dans le cadre d'un procès pénal, sont également de plus en plus employées dans les procès civils, en particulier dans ceux où il s'agit de démontrer une négligence ou un comportement anormal. En Angleterre et aux États-Unis, il est même possible de joindre aux pièces à conviction des séquences vidéo n'ayant pas de rapport direct avec l'affaire, mais pouvant mettre en évidence des éléments permettant de se faire une opinion, par exemple pour montrer le caractère colérique ou violent de l'accusé [1][27].

Il convient de se demander dans quelle mesure de telles preuves sont recevables. Bien sûr, comme d'autres (conversations enregistrées par exemple), les preuves vidéo sont falsifiables, de plus en plus facilement d'ailleurs, avec l'avènement au grand public de techniques de retouche informatique et d'images de synthèse jusqu'ici réservées aux grands studios de production cinématographique (le film "Rising Sun" [10] fournit sur le sujet un scénario intéressant). De telles preuves doivent évidemment être rejetées dans la mesure où on peut prouver la malversation.

Ce qui nous intéresse plus, c'est l'exploitation qui peut être faite de preuves illicites, c'est-à-dire de preuves recueillies en violation d'une règle de droit constitutionnel ou matériel (à opposer aux preuves irrégulières, recueillies en violation d'une règle de procédure). Il s'agit généralement d'une preuve obtenue en violation des règles visant à sauvegarder des droits importants, ceux qui protègent la personnalité ou l'intimité d'une personne, par exemple. C'est précisément ce qu'il peut se produire lors de dérives dans l'usage de la vidéosurveillance. En principe, ce type de preuve doit être retranché du débat. Mais la réalité n'est pas aussi simple.

Domaine pénal.

Prenons le cas de la Suisse. En ce qui concerne le pénal, la jurisprudence du Tribunal Fédérale, qui se base sur les arrêts von Däniken et Schenk [16][17], interdit l'utilisation de preuves illégales. Cependant, ceci ne signifie pas que des vices de forme commis lors de la saisie des moyens de preuve empêchent le juge de se fonder sur de telles preuves.

L'arrêt Schenk, concernant un enregistrement téléphonique recueillie de manière illicite (donc réprimé pénalement), a induit le Tribunal Fédéral à proposer que le juge apprécie les intérêts en présence: dans sa décision de maintenir ou d'écarter la preuve, le juge procède à la balance des intérêts en considérant d'une part l'intérêt public à ce que la vérité soit établie au sujet d'une incrimination grave et d'autre part l'intérêt privé de la personne impliquée à ce que sa sphère personnelle soit sauvegardée.

Les arrêts Schenk et Maître P. [18] excluent tout de même certains procédés absolument prohibés par l'ordre public (contrainte, torture...)

Domaine civil.

Il existe à l'évidence un noyau commun aux dispositions de nature civile ou pénale: l'Etat de droit doit s'accomoder de ce que des règles protectrices du secret peuvent le cas échéant créer des difficultés dans l'établissement de la vérité. Dans la balance des intérêts, la sauvegarde de la vie privée peut prévaloir sur la recherche de la vérité matérielle [19]. Par ailleurs, le juge doit être conscient que la réception de preuves illicites peut encourager à l'avenir la collecte et l'usage de semblables preuves.

L'administration de la preuve dans le domaine civil en Suisse relève essentiellement du droit cantonal. Or les diverses législations cantonales sont muettes quant aux preuves illicites. Quelques solutions jurisprudentielles existent, bien différentes entre elles:

- A Zürich et Berne, il est recommandé au juge de faire la balance des intérêts, ainsi que nous l'avons déjà mentionné pour l'usage de preuves illicites dans le procès pénal [20][21];
- A Genève, la mise en évidence d'une preuve illicite peut mettre en route une procédure annexe, à l'encontre de la source (art 295 al. 2 LPC genevoise) [22];
- Dans l'Etat de Vaud, "le juge civil ne se préoccupe pas qu'une pièce produite aux débats l'aurait été en violation des réserves d'usages" [23][24].

Dans les pays anglophones tels que Etats-Unis, le Canada et l'Angleterre, il est recommandé au juge de faire la balance des intérêts. Les quelques textes et arrêtés y relatifs que nous avons pu consulter montrent que dans l'ensemble, la solution retenue est fort semblable, dans le civil comme dans le pénal (avec toutefois une tendance plus marquée dans le pénal à minimiser la violation de la sphère privée) à celles évoquées en Suisse par les arrêts von Däniken, Schenk et les jurisprudences zürichoises et bernoises. Pour preuve, le cas de l'affaire Richardson contre Davis Wire

Industries Ltd. dans le cas d'un procès civil, déjà mentionnée au sujet de la répression, et fourni en annexe.

Ainsi donc, on voit que non seulement il est difficile de maîtriser l'usage de la vidéosurveillance, souvent par absence de législation adaptée, mais qu'en plus, faire valoir une violation de la sphère privée pour se prémunir contre son usage dans un débat n'apporte généralement pas les résultats escomptés... N'oublions pas que l'oeil de la caméra est finalement beaucoup plus fidèle que celui du témoin oculaire, offrant ainsi beaucoup d'attraits au niveau de la fourniture de preuve.

Analyse

Installation et usage des caméras

La vidéosurveillance est un outil puissant, qui a déjà souvent montré son efficacité. Pour cette seule raison, cette technologie est devenue indispensable aujourd'hui dans une société d'insécurité croissante. Nous avons vu qu'il existe deux formes de vidéosurveillance, l'une de prévention et l'autre de répression.

L'usage de la forme répressive est actuellement trop répandue, exploitée parfois abusivement dans des situations qui ne requiert pas d'en arriver à de telles extrémités. Il serait bon d'étudier davantage l'effet préventif du système. L'individu qui se sent surveillé va modifier son comportement (cf. "Les formes de la vidéosurveillance"). L'aspect préventif pourrait permettre de provoquer ce changement de comportement sans même réaliser de véritable surveillance, en installant de fausses caméras, identiques aux vraies et en annonçant clairement que le local est sous surveillance. Dans le cas de lieux publiques où les risques sont faibles, une telle solution peut sûrement porter ses fruits.

Il est d'autre part essentiel que la législation en vigueur soit complétée afin de limiter les installations "sauvages" de systèmes de vidéosurveillance. Trop souvent, les sociétés privées de gardiennage sont laissées libres à ce sujet. Un bon exemple en matière de limitation est la France, où les installations sont soumises à une réglementation très sévère.

Preuves vidéo dans le domaine de la justice civile et pénale

Il est parfois difficile de contrôler la source d'une preuve, à fortiori d'une preuve vidéo. De plus, ce type de preuve est, avec l'avènement d'outils puissants sur le marché grand public, toujours plus sujet à des manipulations de toutes sortes.

Il serait intéressant de pouvoir authentifier la provenance des sources vidéo utilisées dans des affaires de justice; par exemple, les systèmes vidéo des sociétés de gardiennage devraient générer une signature infalsifiable incluse dans les images, qui authentifie la source et permette de détecter d'éventuelles manipulations extérieures.

Du côté de la cour de justice, on voit bien que l'ajout systématique des preuves vidéo au dossier, avec décision postérieure par le juge ou les jurés de leur pertinence (c'est-à-dire le système à l'américaine) n'est pas idéal, car il peut fossier le débat. On devrait envisager de soumettre de telles preuves à l'examen d'un groupe de spécialistes tant sur le plan technique que juridique, qui déciderait de leur pertinence. Trois critères au moins doivent être envisagés:

- Un critère de qualité des images: est-il possible de distinguer clairement tous les éléments en présence et dans le cas contraire, l'usage de matériel spécialisé, permet-il de faire ressortir clairement les éléments brouillés;

- Un critère de non-unicité: une preuve vidéo ne devrait pas être utilisée seule pour prouver un fait, mais être accompagnée d'autres éléments de preuve;
- Un critère de rapport à l'affaire jugée: vouloir mettre en évidence le caractère d'une personne à l'aide de films vidéo n'ayant aucun rapport devrait être évité autant que possible. Il est facile d'interpréter un comportement de manière erronée.

Les problèmes de qualité des images ont été longuement discutés dans [1].

L'atteinte à la vie privée

Dans le sens inverse, les systèmes de vidéosurveillance sont trop souvent attaqués en exploitant de manière abusive le problème de l'atteinte à la vie privée. L'exemple des affaires Richardson contre Davis Wire Industries Ltd. [2] ou FTMH contre S. [15] le montre bien. Il devrait être prévu que l'on ne peut se retourner contre un exploitant de ces systèmes que dans un cas d'abus manifeste, d'usage illicite des bandes vidéos, etc. dans lesquels un ensemble de preuves tangibles sont susceptibles d'être réunies.

Conclusion

Le domaine de la vidéosurveillance est en forte expansion et le marché est important. Les technologies évoluent très vite. Il est important que la justice étudie de près et rapidement les problèmes liés à ces technologies, afin de se doter d'une législation efficace. Il serait bon également d'obtenir une harmonisation des législations. Lutter contre les dérives, notamment commerciales, est impératif si on veut pouvoir continuer à sauvegarder les libertés fondamentales du citoyen.

Des dérives liées à l'usage des caméras? Que faire alors si on ne peut plus faire confiance aux personnes qui sont censées protéger le citoyen et ses biens? Les préfets en France peuvent déjà contrôler l'usage de ces systèmes. Pourquoi ne pas aller plus loin en installant des caméras dont le rôle serait de surveiller les surveillants...

Bibliographie

1. *Usage of video recordings in surveillance, the value of such as evidence and potential problems which can arise.* 13th Annual BILETA Conference, Trinity College, Dublin, 1998.
2. *Preuve par enregistrement vidéo et droit des employés à la vie privée.* Cabinet Emond-Harnden, 1997. <http://www.emond-harnden.com>
3. *Protection des données à caractère personnel.* Conseil de l'Europe, Direction des Affaires Juridiques, 1987.
4. *La surveillance vidéo: invasion de la vie privée ou réponse raisonnable à l'inconduite?.* Cabinet Emond-Harnden, 1997.
5. *Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.* Journal Officiel du 24 janvier 1995, France
6. *Surveillance et gardiennage: obligation des professionnels.* Véronique Requillard, FACE, avril 1998.
7. *Sécurité privée: silence, on filme.* D. Muller, News d'Ill, janvier 1998
8. DCA, Protection des biens et des personnes. <http://www.dca.com>
9. *Nineteen Eighty-Four*, Georges Orwell, 1946.
10. *Rising Sun*, Michael Backes, Philip Kaufman, 1993.
11. *Sliver*, Ira Levin, 1991.
12. Magazines télévisés: *Le Droit de Savoir* (TF1), *Envoyé Spécial* (France 2), *A Bon Entendeur* (TSR1).
13. Magazine télévisé: *Capital: les supermarchés du futur*, M6.
14. *Councilman Suggests Catching Dog-Doo Lawbreakers on Tape.* CNN Fringe News, mai 1999. <http://www.cnn.com>
15. ATF 114 II 345. FTMH contre S. (Suisse)
16. ATF 96 I 437 = JdT 1972 I 217 (Suisse)
17. ATF 109 la 244 = SJ 1984 p. 153 (Suisse)
18. ATF 117 la 341 = SJ 1992 p. 161 (Suisse)
19. SJ 1987 p. 540 (Suisse)

20. *Kommentar zur Zürcherischen Zivilprozessordnung*, 3^{ème} éd., §140 n°5 et 6. Frank, Sträuli, Messmer.
21. *Grundriss des Zivilprozessrechts*, 3^{ème} éd., chapitre 10 n°101.
22. SJ 1974 p. 97s (Suisse)
23. JdT 1981 III 137 (Suisse)
24. *Procédure civile vaudoise*, 2^{ème} éd., art 170 n°2. Poudret, Wurzbürger, Haldy.
25. JAR 1997 p. 141 (Suisse)
26. *Court decision on hidden devices: parents are free to spy on sitters*. Spy Site, American Innovations, Inc., 1999. <http://www.spysite.com>
27. La justice américaine en direct *live* sur l'internet: <http://www.courttv.com>

Annexes

Extraits de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (France).

Art 10 -I- Les enregistrements visuels de vidéosurveillance ne sont considérés comme des informations nominatives, au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique aux fichiers et aux libertés, que s'ils sont utilisés pour la constitution d'un fichier nominatif.

II - La transmission et l'enregistrement d'images prises sur la voie publique, par le moyen de la vidéosurveillance, peuvent être mis en oeuvre par les autorités publiques compétentes aux fins d'assurer la protection des bâtiments et installations publics et de leurs abords, la sauvegarde des installations utiles à la défense nationale, la régulation du trafic routier, la constatation des infractions aux règles de la circulation ou la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression ou de vol. Il peut être également procédé à ces opérations dans des lieux et établissements ouverts au public particulièrement exposés à des risques d'agression ou de vol, aux fins d'y assurer la sécurité des personnes et des biens. Les opérations de vidéosurveillance de la voie publique sont réalisées de telle sorte qu'elles ne visualisent pas les images de l'intérieur des immeubles d'habitation ni, de façon spécifique, celles de leurs entrées. Le public est informé de manière claire et permanente de l'existence du système de vidéosurveillance et de l'autorité ou de la personne responsable.

III - L'installation d'un système de vidéosurveillance dans le cadre du présent article est subordonnée à une autorisation du représentant de l'Etat dans le département et, à Paris, du préfet de police, donnée, sauf en matière de défense nationale, après avis d'une commission départementale présidée par un magistrat du siège ou un magistrat honoraire.

L'autorisation préfectorale prescrit toutes les précautions utiles, en particulier quant à la qualité des personnes chargées de l'exploitation du système de vidéosurveillance ou visionnant les images et aux mesures à prendre pour assurer le respect des dispositions de la loi. (Dispositions déclarées non conformes à la Constitution par décision du Conseil constitutionnel N°94- .352DC du 8 janvier 1995). Les dispositifs de vidéosurveillance existant à la date d'entrée en vigueur du présent article doivent faire l'objet d'une déclaration valant demande d'autorisation et être mis en conformité avec le présent article dans un délai de six mois.

IV - Hormis le cas d'une enquête de flagrant délit, d'une enquête préliminaire ou d'une information judiciaire, les enregistrements sont détruits dans un délai maximum fixé par l'autorisation. Ce délai ne peut excéder un mois.

V - Toute personne intéressée peut s'adresser au responsable d'un système de vidéosurveillance afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans le délai prévu. Cet accès est de droit. Un refus d'accès peut toutefois être opposé pour un motif tenant à la sûreté de l'Etat, à la défense, à la sécurité publique, au déroulement de procédure engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou au droit des tiers. Toute personne intéressée peut saisir la commission départementale mentionnée au III de toute difficulté tenant au fonctionnement d'un système de vidéosurveillance. Les dispositions du précédent alinéa ne font pas obstacle au droit de la personne intéressée de saisir la juridiction compétente, au besoin en la forme du référé.

VI - Le fait de procéder à des enregistrements de vidéosurveillance sans autorisation, de ne pas les détruire dans le délai prévu, de les falsifier, d'entraver l'action de la commission départementale, de faire accéder des personnes non habilitées aux images ou d'utiliser ces images à d'autres fins que celles pour lesquelles elles sont autorisées est puni de trois ans d'emprisonnement et de 300 000 F d'amende. Sans préjudice des dispositions des articles 226.1 du code pénal et L.120-2, L. 121-8 et L. 432-2-1 du code du travail.

Décret relatif à la vidéosurveillance (Extraits)

Décret n° 96-926 du 17 octobre 1996 relatif à la vidéosurveillance pris pour l'application de l'article 10 de la loi n°95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité.

Art. 1er - La demande d'autorisation préalable à l'installation d'un système de vidéosurveillance dans le cadre de l'article 10 de la loi du 21 janvier 1995 susvisée doit être déposée à la préfecture du lieu d'implantation ou, à Paris, à la préfecture de police, accompagnée d'un dossier administratif et technique comprenant :

1. Un rapport de présentation dans lequel sont exposées les finalités du projet au regard des objectifs définis par ladite loi et les techniques mises en oeuvre, eu égard à la nature de l'activité exercée, aux risques d'agression ou de vol présentés par le lieu ou l'établissement à protéger;
2. Un plan masse des lieux montrant les bâtiments du pétitionnaire et, le cas échéant, ceux appartenant à des tiers qui se trouveraient dans le champ de vision des caméras, avec l'indication de leurs accès et de leurs ouvertures;
3. Un plan de détail à une échelle suffisante montrant le nombre et l'implantation des caméras ainsi que les zones couvertes par celles-ci;
4. La description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images;
5. La description des mesures de sécurité qui seront prises pour la sauvegarde et la protection des images éventuellement enregistrées;
6. Les modalités de l'information du public;
7. Le délai de conservation des images, s'il y a lieu, avec les justifications nécessaires;
8. La désignation de la personne ou du service responsable du système et, s'il s'agit d'une personne ou d'un service différent, la désignation du responsable de sa maintenance, ainsi que toute indication sur la qualité des personnes chargées de l'exploitation du système et susceptibles de visionner les images;
9. Les consignes générales données aux personnes d'exploitation du système pour le fonctionnement de celui-ci et le traitement des images ;
10. Les modalités du droit d'accès des personnes intéressées.

L'autorité préfectorale peut, le cas échéant, demander au pétitionnaire de compléter son dossier. Elle lui délivre un récépissé lors du dépôt du dossier complet.

(...)

Art. 5 - Dans le cas où les informations jointes à la demande d'autorisation ou des informations complémentaires font apparaître que les enregistrements visuels de vidéosurveillance seront utilisés pour la constitution d'un fichier nominatif, l'autorité préfectorale répond au pétitionnaire que la demande doit être adressée à la Commission Nationale de l'Informatique et des Libertés. Il en informe cette commission.

Art. 6 - Dans chaque département, une commission départementale des systèmes de vidéosurveillance est instituée par arrêté du préfet ou, à Paris, du préfet de police.

(...)

Art. 13 - Le titulaire de l'autorisation [prévue à l'article 10 de la loi du 21 janvier 1995] tient un registre mentionnant les enregistrements réalisés, la date de destruction des images et, le cas échéant, la date de leur transmission au parquet.

(...)

Art. 16 - L'autorisation est publiée au Recueil des actes administratifs de la préfecture, sauf dérogation motivée par un impératif de défense nationale. L'autorité préfectorale met à la disposition du public la liste des autorisations publiées des systèmes de vidéosurveillance qui précise pour chacun d'eux la date de son autorisation et le service ou la personne responsable. Elle communique également la liste des systèmes de vidéosurveillance autorisés sur le territoire de chaque commune au maire, qui la met à la disposition du public à la mairie et, le cas échéant, dans les mairies d'arrondissement.

Un cas de litige sur la recevabilité des preuves vidéos obtenues de manière illicite

Cabinet Emond-Harnden, Ottawa, Canada, 1997

La plupart du temps, les arbitres qui doivent décider de la recevabilité des preuves obtenues par la surveillance clandestine des employés appliquent des critères qui visent à pondérer le droit des employés à la vie privée et le droit des employeurs de faire enquête lorsqu'ils soupçonnent la présence d'abus. Un tribunal de la Colombie-Britannique s'est prononcé sur la question et sa décision s'est attirée les louanges des employeurs.

La décision, *Richardson v. Davis Wire Industries Ltd.* (21 avril 1997), portait sur une affaire de renvoi injustifié intentée par un contremaître qui avait été congédié parce qu'il avait dormi au travail et l'avait subséquemment nié. Deux semaines sur trois, M. Richardson était affecté au poste de nuit, de minuit à 7h30. Depuis un certain temps avant le renvoi, l'employeur avait su par d'autres employés que M. Richardson dormait pendant les heures de travail. Plutôt que de confronter M. Richardson directement, l'employeur a préféré faire enquête en installant une caméra cachée dans la salle où les employés prenaient leurs repas.

L'examen de bandes vidéos enregistrées sur une période de plusieurs jours a permis au directeur général de conclure que M. Richardson dormait effectivement au travail. Après avoir encore une fois observé à l'écran que M. Richardson semblait endormi, le directeur général est entré dans la salle et a réveillé M. Richardson brusquement en allumant la lumière. M. Richardson, avant d'être informé de la caméra de surveillance, a nié avoir dormi à d'autres occasions. Il a été congédié sur le champ.

LA PREUVE EST RECEVABLE SI ELLE EST PERTINENTE ET N'ENTRE PAS DANS UNE CATÉGORIE D'EXCLUSION

Lors du procès, l'avocat de M. Richardson a tenté de faire exclure la preuve enregistrée, en soutenant que la décision de faire de la surveillance et la manière d'exécuter cette surveillance étaient toutes deux abusives, et que l'employeur disposait d'autres moyens d'obtenir des preuves contre son employé. L'avocat a également invoqué la *Privacy Act* de la province, qui déclare illicite les violations de la vie privée. L'avocat a concédé le droit de l'employeur de faire enquête, mais ce droit devait être pondéré par l'attente de l'employé qu'il aurait droit à une certaine mesure d'intimité dans la salle des repas.

La décision du tribunal a été défavorable à M. Richardson. Le tribunal a jugé qu'on devait recevoir tout élément de preuve pertinent qui n'entrait pas dans une catégorie d'exclusion. En l'occurrence, la pertinence des éléments de preuve n'était pas en cause puisqu'ils établissaient plusieurs faits importants de l'affaire. On ne pouvait non plus alléguer qu'il fallait exclure les bandes du fait de la violation de la vie privée de l'employé: dans les circonstances, M. Richardson ne pouvait raisonnablement espérer bénéficier d'un droit à la vie privée; néanmoins, même si une telle attente existait, une violation de la *Privacy Act* ne peut quand même pas justifier l'exclusion d'un élément de preuve pertinent:

[TRADUCTION]

"[...] Même si M. Richardson pouvait s'attendre à voir respecter sa vie privée, une violation de la vie privée n'entraîne pas, dans cette affaire, une exclusion des éléments de preuve. La *Privacy Act* ne peut servir que comme fondement à une action en dommages pour délit civil et n'interdit pas la réception d'un élément de preuve, même si cette preuve a été obtenue contrairement à la loi.

M. Richardson ne pouvait raisonnablement s'attendre à ce que l'on respecte sa vie privée alors qu'il dormait pendant ses heures de travail, dans les locaux de la compagnie, et alors qu'il pouvait s'attendre à ce qu'on l'appelle en cas de besoin."

Le tribunal a poursuivi en rejetant l'argument que la surveillance exercée par l'employeur n'avait pas de fondement raisonnable: l'employeur avait pris sa décision en se fondant sur un soupçon raisonnable que M. Richardson dormait alors qu'il était en devoir.

SELON LE TRIBUNAL, LES ACTIONS DE L'EMPLOYEUR SONT REGRETTABLES

Après avoir déclaré la preuve recevable, le tribunal a déploré les méthodes utilisées par l'employeur pour faire enquête sur l'inconduite de M. Richardson. Le tribunal a affirmé que le fait de dormir au travail, bien que puéril et irresponsable, ne méritait quand même pas un congédiement sommaire. En tentant de surprendre l'employé en flagrant délit au moyen d'une caméra cachée, plutôt que d'aborder franchement la question avec lui, l'employeur risquait de miner ses rapports avec ses autres employés:

[TRADUCTION]

"[...] La surveillance [...] est, en elle-même, une pratique qui met en danger les rapports de confiance qui sont tellement essentiels à la relation entre l'employeur et ses employés. Il est malheureux que la compagnie Davis Wire n'ait pas tenté de régler ce problème en confrontant honnêtement M. Richardson avec ses soupçons pour lui dire qu'il était inacceptable de dormir au travail."

Table des matières

INTRODUCTION	3
SOURCES	3
ETAT DE L'ART.....	5
SYSTEMES CLASSIQUES:	5
SYSTEMES DISSIMULÉS:.....	6
LES FORMES DE LA VIDÉOSURVEILLANCE	9
LA PRÉVENTION.....	9
LA RÉPRESSION	10
LES DÉRIVES	13
LES LOIS ET L'ÉTHIQUE	17
PRÉVENTION: LOI OU SIMPLE ÉTHIQUE?	17
REPRESSION: LE PROBLÈME DE L' ATTEINTE À LA VIE PRIVÉE	18
RECEVABILITÉ DES PREUVES OBTENUES PAR VIDÉOSURVEILLANCE	19
<i>Domaine pénal</i>	20
<i>Domaine civil</i>	20
ANALYSE	23
INSTALLATION ET USAGE DES CAMÉRAS.....	23
PREUVES VIDÉO DANS LE DOMAINE DE LA JUSTICE CIVILE ET PÉNALE	23
L' ATTEINTE A LA VIE PRIVÉE.....	24
CONCLUSION	24
BIBLIOGRAPHIE	26
ANNEXES	28
LOI N°95-73 DU 21 JANVIER 1995 RELATIVE À LA SÉCURITÉ (FRANCE).	28
DÉCRET RELATIF À LA VIDÉOSURVEILLANCE (FRANCE)	29
UN CAS DE LITIGE SUR LA RECEVABILITÉ DES PREUVES VIDÉOS OBTENUES DE MANIÈRE ILLICITE.....	30
TABLE DES MATIÈRES.....	33