Mémoire de la
Fédération des travailleurs et
travailleuses du Québec (FTQ)


présenté à la
Commission d'accès à l'information du Québec

sur
l'utilisation de caméras de surveillance
par des organismes publics
dans les lieux publics

Montréal, le 22 septembre 2003

Fédération des travailleurs et travailleuses du Québec
565, boul. Crémazie Est, bureau 12100
Montréal (Québec) H2M 2W3
Téléphone : (514) 383-8000
Télécopie : (514) 383-8001
Site : http://www.ftq.qc.ca

Dépôt légal – 3e trimestre 2003
Bibliothèque nationale du Québec
ISBN 2-89480-140-8

# Table des matières

# Introduction

La Fédération des travailleurs et travailleuses du Québec (FTQ) remercie la Commission d'accès à l'information du Québec de l'opportunité qui lui est offerte de faire valoir son point de vue sur la vidéosurveillance[1]. La centrale intervient parce que les quelque 500 000 travailleurs et travailleuses que nous représentons sont d'abord et avant tout des citoyens et des citoyennes.

Bien que le thème de la consultation ne porte que sur l'usage des caméras de surveillance par les organismes publics, l'accroissement de la vidéosurveillance touche aussi le secteur privé et les milieux de travail. Ainsi, les enjeux et défis à l'égard de la surveillance et de la protection des renseignements personnels qui seront identifiés dans le cadre de cette consultation s'appliqueront vraisemblablement (ou du moins en partie) au secteur privé. C'est pourquoi la FTQ applaudit la tenue d'une telle consultation car nous considérons que l'usage de la vidéosurveillance doit faire l'objet d'une analyse approfondie et d'un large débat au sein de la société québécoise.

La vidéosurveillance est, le plus souvent, implantée dans le cadre d'un programme de prévention de la criminalité ou de renforcement de la sécurité publique. Toutefois, cette surveillance donne lieu à de graves incursions dans la vie privée : en effet, les images captées par les caméras permettent non seulement à l'État mais aussi aux organismes privés oeuvrant dans le domaine de la sécurité de nous identifier. Ces images révèlent notamment des caractéristiques physiques (sexe, voix, agissements, etc.) qui sont uniques et personnelles. La FTQ voit en l'accroissement de la vidéosurveillance une menace certaine à la vie privée. Ainsi, la première partie de ce mémoire présente ce qu'est la vidéosurveillance et brosse aussi un portrait sommaire des principales innovations technologiques qui peuvent rendre la surveillance omniprésente et inopportune. La vigilance étant de mise, la FTQ expose les principaux éléments qui présentent des menaces sérieuses à la protection des renseignements personnels et, conséquemment, militent pour un moratoire sur la multiplication des caméras de surveillance.

Mais plus qu'une question individuelle, la FTQ estime que la vidéosurveillance comporte des enjeux relatifs au maintien d'une société ouverte et démocratique. Comme le souligne avec pertinence le Commissaire à la vie privée du Canada[2], l'usage de la vidéosurveillance pour réduire la criminalité et renforcer la sécurité publique doit être jaugé en tenant compte des valeurs et des objectifs sociaux poursuivis. Les décisions qui découleront de notre réflexion aujourd'hui auront des incidences sur le genre de société que nous voulons, du type de relations que nous souhaitons tisser avec l'État. Or, la FTQ est inquiète que la population québécoise, qui adhère aux valeurs de démocratie et de liberté, ne s'insurge pas davantage contre la vidéosurveillance dont elle fait l'objet

[1] Dans ce mémoire, l'expression « vidéosurveillance » désigne tous les systèmes (caméras de surveillance en circuit fermé (CCTV), caméras biométriques ou numériques, technologies thermales, etc.) qui permettent de photographier l'image d'une personne et les supports techniques et informatiques qui leur sont associés.

[2] Dans son communiqué portant sur les conclusions sur la surveillance vidéo par la GRC à Kelowna, octobre 2001.

notamment, croyons-nous, parce qu'elle en est peu consciente. Dans son ensemble, le mémoire de la FTQ constitue un plaidoyer pour le maintien d'une société moderne et démocratique, respectueuse des droits et des libertés.

# 1. L'essor stupéfiant des nouvelles technologies de surveillance

Depuis les événements du 11 septembre 2001 qui ont amplifié les préoccupations de sécurité à l'échelle mondiale, l'intérêt pour l'usage de caméras de surveillance s'est décuplé. Porté par les innovations technologiques, on assiste à une prolifération de la vidéosurveillance : il existerait plus de 25 millions de caméras de surveillance dans le monde dont 2,5 millions sur le seul territoire de la Grande-Bretagne! Bien qu'à une échelle nettement plus réduite, le Québec n'échappe pas à cette tendance. Les Québécois et Québécoises sont désormais assujettis à une surveillance constante, souvent à leur insu, lorsqu'ils se promènent dans des lieux publics : parcs, stationnements, guichets automatiques des institutions financières, quais de métro, halls d'entrée des édifices provinciaux et municipaux, axes routiers, grands magasins, salles de classe, etc.

Les premières générations de caméras — majoritairement en usage dans ces endroits aujourd'hui — fonctionnent en circuit fermé (*Close Circuit Television ou CCTV)* et sont largement employées pour assurer la sécurité des lieux publics. L'image classique qui nous vient à l'esprit est celle du gardien (gardienne) de sécurité assis devant un nombre impressionnant d'écrans de télévision qui reproduisent les images captées par les caméras stratégiquement disposées pour assurer la sécurité des biens et des personnes. Généralement, ce type de surveillance fonctionne sur un mode essentiellement défensif car les documents vidéos sont consultés ultérieurement au besoin si un méfait a été commis.

Or, grâce à la numérisation, on assiste à une véritable révolution dans la collecte, le stockage et la manipulation des données mais aussi dans les technologies de la vidéosurveillance. Les innovations technologiques seulement dans le domaine de la caméra de surveillance sont effarantes : miniaturisation des caméras, caméras qui pivotent à 360°, dites biométriques qui enregistrent les caractéristiques faciales, à haute-résolution, à vision nocturne, dites électromagnétiques qui « voient » à travers les matières[3], à infrarouges qui détectent des variations de température, à faibles doses de rayons x qui donnent une image du corps et de tout ce qu'il transporte. Ajoutez à ces caméras à la fine pointe de la technologie des zooms puissants, la numérisation de l'image et la transmission d'images par réseau numérique directement à un ordinateur et tous les ingrédients sont réunis pour conférer à la vidéosurveillance un caractère omniprésent et envahissant.

La mise en réseau des caméras à des ordinateurs permet à un seul opérateur de contrôler une multitude de caméras par le simple clic d'une souris. En outre, les images captées par ces caméras peuvent être stockées dans de puissants ordinateurs qui ont la capacité de comparer ces informations avec celles d'autres bases de données (de la police, par exemple), et ce, en temps réel. Contrairement aux données analogiques où la gestion des cassettes est lourde et compliquée, les images sur disques compacts ou DVD peuvent être indexées, ce qui en facilite la recherche. En somme, de nombreux renseignements personnels peuvent être stockés dans de gigantesques bases de

[3] Et peuvent discerner les contours d'une arme dissimulée sous les vêtements.

données, manipulée et analysée à faibles coûts. Dans ce contexte, la protection des renseignements personnels devient un défi de taille.

Les caméras de surveillance ne sont pas en soi tellement menaçantes, mais lorsqu'elles sont couplées à des logiciels dits « intelligents » — présentement, l'industrie de la vidéosurveillance travaille sur un grand nombre de ces logiciels —, elles décuplent les possibilités d'identification et de création de mégabases de données. Par exemple, les images captées par les caméras biométriques pourront être appariées avec des photos numérisées issues de fichiers de malfaiteurs, de personnes recherchées ou de présumés terroristes de la police mais aussi de fichiers administratifs gouvernementaux[4], et ce, à l'aide d'un logiciel de « reconnaissance faciale[5] ». Lorsqu'elle sera au point, cette technologie permettra de créer d'immenses bases de données biométriques. Le logiciel *Automatic Number Plate Recognition Technology*[6] permet d'apparier la photo d'une plaque d'immatriculation aux bases de données administratives qui comportent les informations personnelles présentes sur un permis de conduire : photo, nom, adresse, âge, effractions au code de la route, etc.

Le nec plus ultra dans le domaine de la surveillance sont des logiciels qualifiés de « vision intelligente[7]». Ils renferment des algorithmes[8] de comportements « acceptables» ou « normalisés » et permettant donc d'identifier les comportements « déviants » ou « hors-norme ». *Chromatica*, développé pour améliorer la sécurité des transports en commun, est un de ces logiciels présentement à l'essai dans les métros de Paris, de Londres et de Milan. Par exemple, un passager qui circule à l'inverse du flux normal pourrait être considéré comme s'écartant de la norme donc suspect. Ou encore, un passager qui demeurerait sur le quai après le départ du train déclencherait aussitôt une alarme. En fait, ces logiciels peuvent être « personnalisés » de telle sorte que chaque client détermine les comportements suspects ou dangereux qui susciteront une alerte. Ce logiciel permettra à l'opérateur de la caméra d'analyser les images avec plus d'efficacité.

Deux éléments nous apparaissent particulièrement inquiétants avec le « mariage » des caméras de surveillance et des logiciels dits intelligents. Comme ces dispositifs permettent l'identification et la localisation active des personnes, les caméras de surveillance deviennent donc un outil plus « offensif » pour les personnes responsables de la sécurité (exemple du Super Bowl, voir encadré).
L'autre élément préoccupant, c'est que l'ordinateur se transforme en juge. Dans le cas des logiciels de vision intelligente, qui et comment détermine-t-on un comportement « normal » et, à contrario, un comportement « hors-norme »? Le grand patron de l'entreprise qui développe le logiciel? Le concepteur du logiciel? Un policier à titre de consultant? De plus, qui décide quel est le type de comportement méritant une attention

[4] Au Québec, de telles bases de données existent : les conducteurs possèdent un permis avec photo numérisée et tous les résidents possèdent une carte d'assurance-maladie avec photo.
[5] Il s'agit d'un programme informatique qui analyse les visages captés par les caméras de surveillance.
[6] En usage notamment aux frontières canado-américaines, dans certains États américains et en Grande-Bretagne.
[7] Traduction libre de *Smart vision.*
[8] En anglais, *Pattern-matching algorithms.*

particulière? Les clients qui achètent le logiciel? Toutes ces personnes ont leurs préjugés personnels; elles ont donc leur propre vision de ce qu'est un comportement normal ou acceptable. Pourtant, un comportement peut être non conforme sans être pour autant criminel. Exit les originaux! De toute évidence, ces types de logiciel peuvent devenir un instrument de discrimination en épiant particulièrement les jeunes, les mendiants, les sans abris... bref, tous les groupes marginaux et marginalisés, voire « monsieur et madame tout le monde » qui se permettent un écart de conduite!

Bien que la plupart de ces innovations technologiques ne soient pas encore opérationnelles pour bien des raisons (encore trop coûteux, versions expérimentales, etc.), leur entrée massive sur le lucratif marché privé n'est qu'une question de temps. On le sait, historiquement, toutes les technologies ont été développées pour des fins militaires ou de sécurité publique mais elles ont toujours trouvé un deuxième souffle ou de nouvelles applications au sein d'un service de la police ou des gouvernements. Le secteur privé, qui collabore étroitement avec le secteur militaire dans le développement de ces systèmes de surveillance, offre déjà aux entreprises et aux particuliers — sans nécessairement proposer la toute dernière innovation technologique — des systèmes de surveillance performants. Comme la surveillance est aujourd'hui ancrée dans les mœurs, la population n'hésite pas à se munir de systèmes de surveillance sophistiqués. La production est si volumineuse que les coûts de ces systèmes sont à la baisse. Aujourd'hui, la vidéosurveillance est à la portée de toute personne qui possède quelques centaines de dollars pour acheter le matériel.

S'il y a multiplication des caméras de vidéosurveillance dans les espaces urbains et publics et si on réussit à les relier tous à des systèmes informatiques **opérationnels** d'analyse d'images, on assiste ainsi à la création d'un dispositif qui permet de surveiller n'importe qui en tout temps. L'idée d'un *big brother* qui surveille la société n'est plus de la science-fiction : c'est une possibilité concrète au plan technologique. Bien sûr, « ce n'est pas pour demain la veille » mais la possibilité est bien réelle. Ainsi « se perdre dans la foule » ne signifiera plus rien! Comme il sera démontré plus loin dans ce mémoire, les menaces de tels dispositifs sur la vie privée sont flagrantes.

## SOURIEZ, ON TOURNE!

### EN EUROPE

Le pays qui remporte la palme du plus grand nombre de caméras sur son territoire : la **Grande-Bretagne**! On dit qu'un Londonien se fait photographier en moyenne 300 fois à chaque fois qu'il met le nez dehors.

- Dans le système de transport en commun de Londres, métros et autobus sont équipés de caméras. Près de 450 villes ont mis sur pied un système de vidéosurveillance ratissant soit le centre-ville, parfois même toutes les rues d'une municipalité lorsque celle-ci est petite. Dans le seul quartier de Newham à l'est de Londres, 300 caméras biométriques ont été installées.
- Sur les principales artères de Londres, les caméras épient les chauffards : elles identifient 3 véhicules à la seconde, transmet la photo de l'infraction observée à l'ordinateur. Il refile aussitôt l'identité du propriétaire du véhicule qui reçoit le billet d'infraction même s'il n'est pas le conducteur pris en faute.
- Dans certains guichets bancaires, on trouve à l'essai des caméras qui scrutent l'iris de l'utilisateur, une caractéristique physique aussi fiable que les empreintes digitales. Ainsi, une carte bancaire ou de crédit volée devient inutilisable par la suite pour le fraudeur.

La **France** n'est pas en reste. À l'instar de quelques grandes villes françaises (Paris, Marseille, Lille, Toulon, Montpellier), le centre-ville de Lyon est équipé d'une cinquantaine de caméras sophistiquées (à haute résolution et qui pivotent à 360°). Pour des fins de protection de la vie privée, un logiciel agit pour « masquer » les informations qui proviennent des résidences privées.

### PLUS PRÈS DE NOUS SUR LE CONTINENT...

Les **États-Unis** ont emboîté le pas à la Grand-Bretagne à vitesse grand V.

- La police de la municipalité de Tampa en Floride a installé 12 caméras pour surveiller les personnes et les lieux publics d'un quartier animé de la ville, surtout la nuit. Le logiciel *Face It*, à partir d'une photo, mesure diverses caractéristiques d'un visage comme la distance entre les yeux, la longueur du nez, l'angle de la mâchoire, etc., et crée un profil-type (*template*). L'ordinateur compare ce dernier aux profils présents dans les fichiers de la police et lui donne un taux de ressemblance. Certaines municipalités envisagent de s'engager dans cette voie : Virginia Beach, Palm Springs, Boulder City. Plusieurs casinos utilisent cette technologie pour identifier les tricheurs réguliers et les indésirables.
- Dans le but d'identifier de possibles passagers terroristes, certains aéroports américains — notamment Logan de Boston, F.F. Green à Providence (Rhode Island), San Francisco (Cal.), Palm Beach (Cal.) — utilisent un logiciel de reconnaissance faciale du Département de la défense surnommé *Ferret (*furet en français), mais encore faut-il que les personnes recherchées aient un casier judiciaire.
- Lors de la dernière partie de football américain *Super Bowl*, 100 000 spectateurs ont appris avec stupéfaction qu'ils avaient été filmés à leur insu par des dizaines de caméras toutes reliées au système informatique de la police. À l'aide d'un logiciel de reconnaissance faciale, les images captées ont ainsi été analysées par ordinateur et couplées aux informations des fichiers policiers en temps réel. Selon les autorités policières, 19 personnes suspectes, c'est-à-dire recherchées par la police ou ayant un casier judiciaire, ont été identifiées grâce à cette technologie.
- Et le nec plus ultra : le *Combat Zones That See* (CTS). Ce projet chapeauté par le *US Defense Advanced Research Projects Agency* a pour objectif de surveiller « tout ce qui bouge » dans les villes étrangères afin de protéger les troupes militaires américaines postées dans le monde. Concrètement, il s'agit d'un système de surveillance qui utilisera un important réseau de caméras et d'ordinateurs pour pister, enregistrer et analyser les mouvements de tous les véhicules circulant dans une ville occupée. Le « joyau » de ce système est un logiciel innovateur capable de déterminer les types de véhicule selon la couleur, la taille et la forme, de lire les plaques d'immatriculation, d'identifier, à l'aide de la biométrie, les conducteurs et leurs passagers, et d'analyser les mouvements « normaux » ou non. Les premiers tests sont prévus pour septembre.
- Outre les exemples qui concernent les lieux publics, le territoire américain est aussi la mecque des webcams où, grâce à Internet, l'intimité des foyers n'a plus de secret. On n'a qu'à penser aux *nannycams* qui permettent aux parents de surveiller leurs enfants à la maison ou à la garderie depuis leur lieu de travail ou l'endroit où ils se situent dans le monde, et ce, en temps réel.

## SOURIEZ, ON TOURNE! (SUITE)

### ET À L'ÉCHELLE PLANÉTAIRE…

**Échelon** : Il s'agit d'un dispositif de surveillance électronique mis sur pied par les services de renseignements de États-Unis, de la Grande-Bretagne, du Canada, de l'Australie et de la Nouvelle-Zélande. Ce système peut intercepter deux millions de conversations à la minute : conversations téléphoniques, cellulaires, fax, courrier électronique. Un peu à l'image d'un moteur de recherche (Google, AltaVista) qui fouille Internet à partir d'un mot ou d'une expression, des logiciels sophistiqués analysent les conversations interceptées à partir de mots-clés ou adresses fournis par les gouvernements concernés.

* * *

Qu'arrive-t-il si une personne envoie un courriel à son amoureux comportant des propos lubriques (voire pornographiques) tout à fait acceptables dans le domaine de la vie privée mais prenant une toute autre dimension dans le champ public? Si, lors d'un appel téléphonique par cellulaire, une personne exprime son mécontentement à l'égard de son patron en des termes pas trop flatteurs? Au Québec, la mésaventure d'une haute-fonctionnaire qui a exprimé une opinion à l'égard de certains personnages politiques a vécu des moments très inconfortables lorsque ses propos sont tombés dans le domaine public.

*Big brother* vous avez-dit? Si aujourd'hui, nous ne pouvons plus nous exprimer... bientôt peut-être ne pourrons-nous plus penser?

# 2. Deux valeurs qui s'entrechoquent

Les deux grandes valeurs que l'on doit considérer dans l'analyse de l'utilisation des caméras de surveillance sont la sécurité et la vie privée. Souvent présenté comme une nécessité pour assurer la sécurité de la population, le recours aux caméras de surveillance a de graves incidences sur le droit à la vie privée. Et le renforcement de l'un se réalise souvent au détriment de l'autre : où trouver l'équilibre?

## 2.1. *BIG BROTHER* : AU NOM DE LA SECURITE PUBLIQUE...

Il est accepté que l'État assure la sécurité publique, la protection des personnes et sa propre sécurité. Les caméras de surveillance sont aujourd'hui un des éléments qui composent la boîte à outils des organismes publics permettant d'atteindre ces objectifs. Au Québec, les principaux systèmes de surveillance par caméras implantés par les corps policiers répondent à des impératifs de sécurité, de protection de la population et de lutte au sentiment d'insécurité : prévenir les vols, les actes de vandalisme et les activités criminelles, combattre la délinquance dans les parcs urbains et les rues commerçantes, etc. Certains ministères et organismes publics (municipalités, écoles et cégeps, centres hospitaliers, sociétés de transport, etc.) ont aussi recours aux caméras de surveillance pour éviter les dommages à leurs propriétés et assurer la sécurité des usagers et des usagères. Dans ces derniers cas, ce sont les garages, les stationnements, les lieux d'accès (portes, halls d'entrée, couloirs, escaliers, etc.), salles diverses (bibliothèques, salles de classes, etc.) qui sont contrôlés par les caméras de surveillance. On invoque aussi, mais dans une moindre mesure, des raisons d'efficacité et d'économie de coûts pour justifier l'usage des caméras de surveillance.

Ainsi, l'usage de plus en plus répandu des caméras de surveillance semble être une réponse à la hausse alléguée de la criminalité et au sentiment d'insécurité de la population. Pourtant, les plus récentes données de Statistique Canada montrent que le taux de criminalité global[9] du Canada a poursuivi la tendance à la baisse amorcée depuis 1990 et avoisinait, en 2002, le taux enregistré en1979. Le Québec suit la tendance et affiche le taux le plus bas des provinces canadiennes à ce chapitre. Ce phénomène observé au Canada et au Québec s'inscrit dans le même contexte que plusieurs pays industrialisés affichant une diminution de leur taux global de criminalité au cours des dernières années. Quoiqu'il s'agisse d'un phénomène complexe à analyser, le principal facteur évoqué pour expliquer le recul de la criminalité est le vieillissement de la population[10], l'hypothèse étant que les jeunes sont plus portés à commettre des actes criminels. Malgré un bilan plutôt positif en termes de criminalité, paradoxalement, les citoyens et les citoyennes expriment un sentiment grandissant d'insécurité[11]. L'écart entre la perception d'insécurité qui anime la population et le recul de la criminalité

[9] Canada : 8 386,6 crimes pour 100 000 habitants (Québec : 6 392,1). Taux d'homicides : Canada a 1,9 pour 100 000 habitants, alors que le Québec en enregistre 1,6. Les crimes contre la propriété représentent la majorité des infractions.

[10] Toujours selon Statistique Canada, mais dans une moindre mesure, l'éducation, le chômage, la transformation des structures familiales et la consommation de drogues sont aussi des facteurs qui influencent la criminalité.

[11] Tendance confirmée par une enquête de Statistique Canada (août 2002) et une étude du Conseil canadien de développement social (juillet 2002) sur la perception de la population à l'égard de la sécurité.

étonne. Or, selon un criminaliste et professeur à l'Université de Montréal, les deux phénomènes seraient interreliés : « plus on est vieux, plus on est peureux. Et plus on est vieux, moins on commet de crime également[12] ». Il semble aussi que les médias contribuent également au sentiment d'insécurité de la population en rapportant beaucoup plus qu'avant les faits divers et en offrant une couverture étendue aux crimes à sensation. L'utilisation des caméras de surveillance pour combattre le sentiment d'insécurité ne nous apparaît pas la meilleure voie à suivre.

## 2.2. … MAIS AU PERIL DE LA VIE PRIVEE ET DE LA LIBERTE?

Mais quels sont les impacts de cette vidéosurveillance sur la vie des gens? Avant d'aborder cette question, un détour sur ce que sont la vie privée et la liberté s'impose.

Aujourd'hui, les Québécois et les Québécoises vaquent à leurs occupations et déambulent dans les endroits publics sans se soucier d'être constamment surveillés. C'est qu'ils ont la conviction profonde d'évoluer dans une société démocratique, libre et ouverte où le droit à la vie privée[13] est protégé par différentes lois et où une personne peut se trouver dans un endroit public et prétendre à un espace de vie privée. Toutefois, tout droit a ses limites et peut être restreint lorsque l'intérêt collectif est en jeu. Il s'agit donc de trouver un juste équilibre entre les obligations de la vie en société et le droit à la vie privée. Un ancien juge de la Cour suprême affirme même que « la notion de vie privée est au cœur de la liberté dans un État moderne»[14]. Ainsi, étroitement interrelié avec celui de la liberté, le droit à la vie privée constitue une valeur humaine fondamentale.

C'est ce juste équilibre entre nos droits et nos obligations que nous avons réussi à bâtir collectivement au Québec au cours des années, de sorte que le droit à la vie privée et la protection des renseignements personnels sont assurés par plusieurs outils législatifs[15] dont trois spécifiquement québécois : la *Charte des droits et libertés de la personne*, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (« Loi sur l'accès ») et la *Loi sur la protection des renseignements personnels dans le secteur privé* (« Loi sur le secteur privé »).

On constate par ailleurs que la population est en général assez indifférente à la surveillance dont elle fait l'objet. On entend souvent des citoyens et citoyennes émettrent le commentaire suivant : *« Moi, je ne m'oppose pas aux caméras : je n'ai rien à cacher! Au contraire, leur présence me rassure. Si elles permettent aux policiers de pouvoir arrêter les malfaiteurs, pourquoi pas? »*. Bien qu'il traduise une réaction bien humaine, ce raisonnement est inquiétant. En fait, les individus expriment qu'ils ne se

---

[12] Maurice Cusson, Le Devoir, 25 juillet 2003.

[13] Bien que le droit à la vie privée soit un concept difficile à cerner, il vise essentiellement à protéger la personne dans son intégrité, sa dignité et sa liberté. Ce concept comprend notamment le droit à l'anonymat et à l'intimité, le droit à l'aménagement de sa vie personnelle et familiale, le droit au secret et à la confidentialité.

[14] Juge La Forest dans l'arrêt R.c. Dyment, 1988.

[15] S'ajoute le *Code civil du Québec*, la *Loi sur la protection des renseignements personnels et les documents électroniques* (loi fédérale), la *Charte canadienne des droits et libertés* et le *Code criminel*.

sentent pas du tout concernés par cette surveillance. Aujourd'hui, la population trouve normale et acceptable l'utilisation des caméras pour protéger ses biens et se sécuriser. Par exemple, les personnes qui utilisent les stationnements sous-terrains se sentent rassurés à l'idée qu'un agent de sécurité surveille leurs déplacements et puisse leur venir en aide en cas de pépins. Les résidents des habitations à loyer modique trouvent acceptables d'être surveillés par des caméras de surveillance pour contrer les actes de vandalisme sur leurs terrains et dans leur bâtisse. Bref, en s'implantant subrepticement dans tous les aspects de la vie quotidienne, on a banalisé la vidéosurveillance.

Pour la FTQ, vivre dans une société libre, c'est avoir la liberté de penser et d'agir sans craindre d'être systématiquement observé. Or, les caméras de surveillance observent tout le monde et pas seulement les malfaiteurs : comment peut-on accepter d'être considérés comme de présumés suspects lors de toutes nos sorties dans tous les lieux publics? Les caméras ouvrent la porte à une forme de surveillance continue qui est incompatible avec le maintien d'une société ouverte et démocratique. C'est la valeur fondamentale du droit à la vie privée, essentielle à la liberté des personnes, qui est mise aussi en cause par les avancées technologiques notamment en matière de surveillance mais dans tous les autres domaines[16].

Malgré la baisse généralisée des taux de criminalité, certains individus croient que la perte de liberté et les restrictions du droit à la vie privée sont le prix à payer pour se protéger de la criminalité. Pourtant, comme il le sera démontré plus loin dans ce mémoire, l'efficacité de cette technologie pour lutter contre la délinquance et la criminalité n'a pas été démontrée. De plus, l'absence de criminalité ne se traduit pas nécessairement par une amélioration de la qualité de vie en société. Cela ressemble davantage à un État policier ou à une société sous constante surveillance. L'enjeu du débat aujourd'hui est le suivant : quel type de société voulons-nous?

[16] L'Internet et le courriel facilitent l'invasion de la vie privée.

# 3. Non au recours systématique aux caméras!

Les promoteurs de la vidéosurveillance estiment que celle-ci décourage les malfaiteurs, réduit les activités criminelles et accroît le sentiment de sécurité des citoyens et des citoyennes qui circulent dans des lieux publics. On prétend également que les innovations technologiques améliorent l'efficience des caméras comme outils de prévention de la criminalité. Notre réflexion sur la vidéosurveillance nous conduits à nous inscrire en faux à l'égard de cette analyse. Par conséquent, tout en reconnaissant que dans des certains cas exceptionnels (menaces d'actes violents ou réunions ministérielles internationales justifiant des mesures de protections exceptionnelles) ou endroits publics particulièrement vulnérables (ex. : parlement, ministères, etc.) où l'utilisation des caméras de surveillance est indiquée, nous nous opposons à un usage systématique et grandissant des caméras de surveillance au Québec dans les lieux publics.

## 3.1. INEFFICACES POUR COMBATTRE LA CRIMINALITE

Le premier argument qui milite pour l'usage de caméras de surveillance — fortement répandu dans la population y compris au sein de nos membres — c'est que cette surveillance est sensée nous protéger et surtout contrer la criminalité. Pourtant, si certaines municipalités affirment haut et fort avoir abaissé leur taux de criminalité grâce aux caméras, ces affirmations doivent être considérées avec la plus grande prudence. À ce jour, aucune étude n'a démontré de façon concluante que les caméras de surveillance étaient efficaces pour lutter contre la délinquance et la criminalité. Souvent, les données recueillies par les corps policiers de la municipalité sont partielles et anecdotiques. Une étude[17] montre qu'une fois ajustées, les données pour prendre en compte la tendance générale à la baisse de la criminalité ne confirment pas que les caméras ont un impact significatif sur la prévention et la réduction de la criminalité. En outre, lorsque les statistiques sont ventilées selon les différents types de méfaits, on note que la petite criminalité (vol, vandalisme, ébriété, revente de drogues, etc.) est à la baisse alors que les crimes avec violence augmentent. Les chercheurs ont aussi constaté que la présence de caméras de surveillance a souvent entraîné un déplacement des problèmes de criminalité et de délinquance vers des secteurs non exposés au « regard » de la caméra. Enfin, la prise en compte d'autres facteurs telles la revitalisation d'un centre-ville qui s'accompagne d'une installation de caméras nuance l'impact des caméras : la chute des taux de criminalité est davantage liée à la revitalisation qu'à la vidéosurveillance.

En ce qui concerne l'efficacité et les coûts moindres, nous doutons de la pertinence de ces arguments. Selon le Commissaire à la vie privée du Canada, la poursuite de ces objectifs a eu des effets négatifs sur la prestation policière. En effet, suite aux restrictions budgétaires qui ont été imposées dans le passé, on constate que la présence des caméras s'est substituée aux patrouilles policières dans les endroits publics au lieu d'être en soutien à leur travail. Pourtant, les possibilités d'intervention d'un policier qui observe un écran situé à des kilomètres de l'endroit où se produit le délit ou l'agression

[17] Effectuée par le *Scottish Office Central Research Unit,* « Crime and Criminal Justice Research Findings No 30 », juillet 1999, 5 pages.

sont plutôt limitées, laissant planer un doute sur les réels gains d'efficacité à protéger la population.

Force est de constater que ce discours sur l'efficacité de la vidéosurveillance est véhiculé par certaines autorités gouvernementales (le gouvernement britannique finance l'installation de systèmes de surveillance et alloue un budget de fonctionnement pour les municipalités qui le désirent), par les corps policiers et par les entreprises privées dont la principale mission (et source de profits) est la vidéosurveillance. En réponse aux critiques, ces derniers affirment rechercher l'effet de dissuasion voire décourager les activités criminelles avant qu'elles ne se produisent. Néanmoins, un malfaiteur bien décidé à commettre un vol dans une banque se moque de la présence de la caméra et utilise souvent une cagoule pour cacher son identité. Même si on adhère à l'idée que la présence des caméras peut avoir un impact dissuasif, les données empiriques en termes de réduction réelle d'actes criminels ne le confirment pas. Les caméras de surveillance réussissent-elles à atténuer le sentiment d'insécurité de la population? Si c'est le cas, il s'agit d'un faux sentiment de sécurité parce que concrètement, la vidéosurveillance n'assure pas une protection accrue de la personne. Enfin, selon le service de police de Montréal, d'autres éléments peuvent atténuer le sentiment d'insécurité : effacer les graffitis, éliminer les grossièretés, minimiser la revente de drogues, etc. Tous ces objectifs peuvent être atteints sans nécessairement recourir à une caméra de surveillance.

## 3.2. LES RISQUES DE DERAPAGES ET D'ABUS SONT GRANDS

Selon les études consultées, il apparaît que les logiciels « intelligents » ne sont pas encore au point. Une étude du Département américain de la défense a montré que les logiciels de reconnaissance faciale montraient un haut taux d'appariement de « faux-positifs » c'est-à-dire que le visage d'une personne innocente avait été malencontreusement apparié avec un des présumés terroristes présents dans le fichier gouvernemental ainsi que de nombreux appariements « faux-négatifs », c'est-à-dire que le logiciel n'était pas parvenu à identifier le visage d'un terroriste qui comptait parmi les visages contenus dans la base de données. Cela a pour effet de cibler un grand nombre de personnes innocentes et de « rater » les personnes réellement soupçonnées de délits. L'objectif premier visé par ce logiciel n'est donc pas atteint. Et nous pouvons aisément imaginer les conséquences énormes et dommageables d'un faux-appariement pour une personne innocente. De plus, les ressources policières allouées pour contrôler les faux-négatifs sont autant de ressources qui ne sont pas canalisées dans des approches alternatives plus efficaces. Mais prenons garde : un de ces jours, ces logiciels seront opérationnels; nous devrons alors composer avec leur caractère très envahissant au plan de la vie privée.

La constitution de mégafichiers de données biométriques qui résulteront de cette vidéosurveillance comporte aussi d'énormes risques d'abus et de dérapages. Leur création commande une vigilance de tous les instants de la part des citoyens et des citoyennes pour s'assurer de la fiabilité des renseignements contenus dans la base et de l'usage de ces derniers par autrui. L'histoire nous enseigne aussi que des renseignements personnels colligés dans un but précis au départ ont été utilisés à

d'autres fins. Par exemple, certaines personnes qui ont accès à l'information contenue dans ces banques de données pourraient être fortement tentées de faire un usage frauduleux de ces renseignements. On n'a qu'à penser au cas québécois d'une employée d'une entreprise mandataire de la Société de l'assurance automobile du Québec (SAAQ) qui a exploré leur banque de données pour recueillir des informations sur des personnes visées par un groupe de motards. Cet accès illégal à des renseignements personnels a été fatal pour trois d'entre elles. On peut à peine imaginer les possibilités de fraudes liées à une mégabase de données biométriques si ces dernières tombent entre les mains d'un employé sans scrupules. Ces mégafichiers posent des problèmes sérieux de contrôle et de protection des renseignements.

## 3.3. TOUT ÇA A QUEL PRIX? AU DETRIMENT DE LA VIE PRIVEE

Depuis plusieurs années, on assiste à un glissement : les caméras qui, au départ, devaient servir à renforcer la sécurité sont en pratique devenues des outils de contrôle de la société. Si nous nous savons filmés en tout temps lors de nos sorties dans des lieux publics ou si nous avons le sentiment d'être épiés lorsque nous circulons en ville, il est évident que cette conscience teintera nos agissements. Une société sous surveillance modifie de façon subtile mais profonde les comportements des gens. Étant conscients des activités de surveillance, l'État n'a plus besoin de réellement contrôler les citoyens et les citoyennes parce que ceux-ci se « contrôlent » eux-mêmes se sachant surveillés. Ils adoptent des comportements *politically correct*. Dans un autre ordre d'idée, ils seront possiblement réticents à afficher en public une dissidence ou même à participer à des manifestations au risque d'être identifiés et fichés dans des bases de données. Il s'agit là de graves intrusions dans la vie privée et les libertés individuelles.

D'un point de vue sociologique, les caméras de surveillance suscitent d'autres types de dérapage. Un des enjeux de la vidéosurveillance concerne le pouvoir : qui et quel comportement surveille-t-on? Une étude britannique[18] qui a analysé un échantillon comprenant plus de 600 heures d'enregistrement vidéo montre que sans directives précises, les opérateurs des caméras — généralement de sexe masculin et de couleur blanche — ciblaient les groupes sociaux qui leur semblaient les plus susceptibles d'avoir des comportements déviants. Ainsi, ils avaient tendance à cibler de façon disproportionnée (en regard à leur présence dans la population totale) les hommes, jeunes et de couleur. En général, près de quatre personnes sur dix étaient surveillées pour « aucune raison évidente » (c'est-à-dire ayant des comportements louches pouvant mener à une tentative de vol ou de vandalisme, etc.). D'autres études indiquent que les opérateurs de caméra — des êtres humains qui viennent au travail avec leurs préjugés, leurs travers et aussi leurs intérêts personnels — consacraient environ 15 % de leur temps à regarder les femmes, et ce, pour d'autres raisons que celles liées au contrôle de la criminalité!

Ce qui est déplorable avec l'usage de la vidéosurveillance, c'est qu'on axe tous les rapports entre les citoyens entre eux mais aussi entre la population et l'État sur la

[18] Norris, Clive et Gary Armstrong, « *The maximum surveillance society, The Rise of CCTV* », Berg Oxford, Royaume-Uni, 1999, 248 pages.

répression. Il importe donc d'envisager des alternatives à la vidéosurveillance qui mettraient, par exemple, l'accent sur la prévention, la réinsertion, le réaménagement des lieux publics (meilleur éclairage, aménagement d'un parc, etc.). Nous sommes d'avis que l'utilisation de la vidéosurveillance pour lutter contre la délinquance chez les jeunes est un moyen disproportionné et inadéquat. Dans ce cas précis, des alternatives telles la création d'un centre de loisirs ou la mise sur pied d'un programme d'intervention auprès des jeunes en difficultés risquent d'avoir de bien meilleurs résultats tout en étant moins envahissantes au chapitre de la vie privée.

## 3.4. TRAVAILLEURS ET TRAVAILLEUSES SOUS SURVEILLANCE AUSSI?

En ce qui concerne les organismes publics, le principal usage de la vidéosurveillance concerne essentiellement la protection de la propriété et des biens matériels. Toutefois, cette surveillance ne s'arrête pas qu'aux biens : les caméras captent forcément les faits et gestes des travailleurs et des travailleuses sur leurs lieux de travail. En théorie, l'existence des caméras n'avait pas pour objectif premier d'observer et de contrôler le travail, mais un glissement est toujours possible. Comment peut-on s'assurer que les caméras de surveillance ne seront pas utilisées à d'autres fins comme contrôler les employés dans leur travail? Ou que les images ne seront pas utilisées à des fins disciplinaires? Les conséquences de se savoir constamment épié dans le cadre de son travail auront vraisemblablement des effets négatifs sur notre qualité de vie au travail.

Outre l'angle « contrôle du travail » de la vidéosurveillance, cette dernière a aussi de graves incidences sur la vie privée des travailleurs et des travailleuses. En effet, certaines commissions scolaires et entreprises privées qui soupçonnaient la présence de trafic de drogues dans leurs établissements ont installé des caméras de surveillance dans les toilettes, endroit privilégié pour ce genre d'activité. Cependant, tous les employés, et non seulement les revendeurs, ont été surveillés et ont subi une grave intrusion dans leur vie privée. Nous sommes d'avis qu'aucun motif n'est suffisant pour permettre l'utilisation de caméras de surveillance dans les toilettes. Si des présomptions de comportement criminel existent, les dirigeants de ces organismes publics et de ces entreprises, comme tout citoyen, devraient faire appel aux services policiers pour corriger la situation.

La vidéosurveillance des employés dans leurs milieux de travail ne date pas d'hier mais elle est, aujourd'hui, plus systématique. Dans les milieux de travail syndiqués, des dispositions de la convention collective peuvent restreindre grandement ce type de surveillance et assurer qu'elle ne porte pas atteinte à la vie privée ou à la dignité des travailleurs et des travailleuses. Il est tout à fait normal qu'une personne ait des activités privées au travail, et cet espace de vie privée au travail a été reconnu par différents jugements. Si la surveillance mine le droit à la vie privée du travailleur et de la travailleuse, elle constitue une condition de travail injuste et déraisonnable.

# 4. Recommandations

Les citoyens et les citoyennes ne mesurent pas toujours l'ampleur du pouvoir et les possibilités de contrôle que donnent les technologies de surveillance à l'État. Les seuls garde-fous contre un usage abusif de ces technologies de surveillance sont les lois et les institutions gouvernementales qui sont en place, dont la Commission de l'accès à l'information (CAI). Nous félicitons la CAI pour les efforts réalisés à ce jour pour baliser l'usage des caméras de surveillance, notamment la formulation des dix règles minimales. Le lecteur trouvera copie de ces règles minimales en annexe. Toutefois, comme vous le mentionnez avec pertinence, il s'agit d'un minimum. Nous espérons vivement que les recommandations suivantes se refléteront dans les nouvelles directives ou dans une future politique gouvernementale que vous élaborerez au terme de cette consultation.

### 1RE RECOMMANDATION : UNE CAMPAGNE D'EDUCATION POPULAIRE

Compte tenu du manque d'information et souvent de l'indifférence de la population à l'égard de la vidéosurveillance et ses conséquences, il nous apparaît urgent que la Commission de l'accès à l'information fasse une campagne de sensibilisation énonçant les menaces de la vidéosurveillance sur le droit à la vie privée et permettant de mieux faire connaître les droits et les recours de la population en matière de renseignements personnels.

### 2E RECOMMANDATION : RESTREINDRE L'UTILISATION DES CAMERAS

La FTQ ne peut donner son appui à une érosion du droit à la vie privée, ce droit étant essentiel au maintien de la dignité et de la liberté de toute personne. Ainsi, la centrale fait sienne la position développée par le Commissaire à la protection de la vie privée du Canada qui affirme que « la seule façon efficace de prévenir [la surveillance/identification] consiste tout d'abord à empêcher la prolifération des caméras de surveillance »[19]. En réponse à la première question posée dans le document de réflexion soit *« de déterminer, préalablement, si l'utilisation de caméras de surveillance est <u>nécessaire</u> et pas simplement utile »*, nous croyons que les caméras de surveillance ne devraient être justifiées que dans certaines situations exceptionnelles et temporaires.

Cela dit, la FTQ reconnaît que le recours aux caméras est déjà très répandu dans les organismes publics et est parfois nécessaire dans des situations où les contraintes sont telles que l'intervention policière traditionnelle est impossible. Il est donc important d'en baliser l'usage par les corps policiers et par les agents responsables de la sécurité. Inspirée par les dix règles minimales d'utilisation des caméras de surveillance définies par la CAI, la FTQ a développé les recommandations suivantes. Comme nous souhaitons restreindre l'usage des caméras de surveillance, nous n'avons pas jugé bon

[19] Commissariat à la protection à la vie privée du Canada, *Communiqué : Le Commissaire à la protection à la vie privée rend publiques ses conclusions sur la surveillance vidéo par la GRC à Kelowna*, 14 octobre 2001.

de nous pencher sur chacune de ces règles. Nous nous sommes plutôt concentrés sur trois d'entre elle parce qu'elles constituent, selon nous, l'enjeu de fond.

***Avant même l'utilisation d'un système de surveillance :***

Nous devons collectivement nous poser la question suivante : quel prix sommes-nous prêts à payer pour assurer notre sécurité? Avant même d'envisager l'utilisation d'un système de vidéosurveillance, cette approche doit être mise en comparaison avec des solutions alternatives. L'usage des caméras de surveillance ne devrait être retenu que si et seulement si les bénéfices en matière de sécurité accrue surpassent l'érosion du droit à la vie privée.

## 3E RECOMMANDATION : ANALYSE DE LA CRIMINALITE OU DES BESOINS DE SECURITE

1. Nous sommes d'accord avec la Commission qui propose la réalisation d'études indépendantes et d'analyses de la criminalité afin d'évaluer les risques qu'une infraction ou qu'un méfait soit commis ou sur l'évaluation des dangers en matière de sécurité et de protection de la population. Ces études devraient pouvoir identifier et évaluer les besoins.

2. Une fois les objectifs et les besoins identifiés, il faudra examiner chacune des solutions disponibles, leurs coûts, leurs implications socioéconomiques et leurs impacts sur les droits des personnes, et ne retenir que les solutions les moins envahissantes au chapitre de la vie privée. Le principe qui devrait nous guider : un juste équilibre entre qualité de vie et répression de la criminalité par la surveillance. Et, si les caméras sont retenues, ces études devront énumérer les motifs qui en justifient l'utilisation et faire la preuve que la vidéosurveillance permettra d'atteindre les objectifs visés.

***Si les caméras sont retenues comme outils de surveillance :***

## 4E RECOMMANDATION : APPLICATION DES REGLES MINIMALES

En attendant l'élaboration d'une future politique gouvernementale en matière d'utilisation des caméras de surveillance, les dix règles minimales de la CAI devraient être appliquées rigoureusement par tous les organismes publics.

De plus, nous suggérons à la CAI d'introduire dans ses règles minimales, la création d'un comité d'éthique composé de représentants de la population et de l'organisme utilisateur. Sans nous pencher sur toutes les modalités de fonctionnement, ce comité aurait pour principal mandat de discuter de toutes les questions relatives à la protection de la vie privée et de s'assurer d'un usage rigoureux des caméras de surveillance conforme aux directives de la CAI.

## 5E RECOMMANDATION : REEXAMEN POUR LES SYSTEMES EXISTANTS

Les données fournies par la CAI montrent que les caméras de surveillance sont assez courantes au sein des organismes publics. Nous recommandons que ces organismes procèdent à un réexamen de leurs systèmes de vidéosurveillance — en tenant compte des directives émises dans la recommandations trois —, évaluent la pertinence de maintenir le fonctionnement des caméras et, dans certains cas, d'envisager la possibilité de mettre fin à leur utilisation.

## 6E RECOMMANDATION : NON AUX ENORMES BASES DE DONNEES

Considérant que les risques d'abus et de dérapages sont considérables, la FTQ s'oppose vivement à la création de fichiers de données biométriques qui peuvent rapidement ficher l'ensemble de la population. Dans sa collecte de renseignements, les organismes gouvernementaux doivent envisager d'autres solutions qui offriront une alternative valable sans faire entorse au respect de la vie privée. Pris sous cet angle, il est clair que nous nous opposons à l'appariement des fichiers administratifs ainsi qu'aux associations d'images avec les données biométriques.

## 7E RECOMMANDATION : CONTROLER AUSSI LES MILIEUX DE TRAVAIL

La FTQ est très préoccupée par l'accroissement de la vidéosurveillance qui touche les milieux de travail. En effet, l'application de technologies de surveillance de plus en plus sophistiquées émousse la frontière entre la vie privée au travail et le travail lui-même. Il est donc pressant de s'interroger collectivement sur les limites de la vidéosurveillance des lieux de travail et sur son caractère acceptable comme outil de gestion. Nous demandons donc à la Commission de l'accès à l'information de tenir une autre consultation afin de dégager les grandes pistes visant à baliser l'usage de la vidéosurveillance dans les milieux de travail.

Annexe (1)

LC/fv
sepb-57
2003-08-27