

## Services aux organisations

### **La Commission d'accès à l'information du Québec face à la vidéosurveillance des lieux publics par les organismes publics**

*Présenté à  
La Commission d'accès à l'information*

*Étude produite par  
Christian Boudreau et Marie-Claude Prémont  
Professeurs à l'ENAP*

Juin 2009





## TABLE DES MATIÈRES

<b>1. SOMMAIRE</b> .....	<b>1</b>
<b>2. INTRODUCTION</b> .....	<b>5</b>
<b>3. ANALYSE COMPARÉE DES GUIDES D'UTILISATION DE LA VIDÉOSURVEILLANCE DANS LES LIEUX PUBLICS AU CANADA</b> .....	<b>7</b>
3.1. LA NÉCESSITÉ ET LA PROPORTIONNALITÉ .....	10
3.2. LA GESTION DES IMAGES ET DES ENREGISTREMENTS.....	10
3.3. LA LÉGITIMITÉ ET LA RESPONSABILITÉ .....	11
3.4. L'ÉVALUATION ET LA VÉRIFICATION PÉRIODIQUES .....	11
3.5. LA DÉMARCHE ET LA TRANSPARENCE .....	12
3.6. SOMMAIRE DE L'ANALYSE COMPARATIVE DES GUIDES DU CANADA .....	12
<b>4. EXAMEN DE TROIS PROJETS DE VIDÉOSURVEILLANCE AYANT FAIT L'OBJET D'ENQUÊTE PAR LA CAI</b> .....	<b>14</b>
4.1. DESCRIPTION SOMMAIRE DES PROJETS ET DE LA SURVEILLANCE EXERCÉE PAR LA CAI .....	14
4.1.1. <i>Centre-ville de Sherbrooke</i> .....	14
4.1.2. <i>Centre-ville de Baie-Comeau</i> .....	16
4.1.3. <i>Centre-ville de Montréal</i> .....	19
4.2. QUELQUES CONSTATS SUR LES TROIS PROJETS.....	24
4.2.1. <i>Un contexte économique et social favorable à la vidéosurveillance</i> .....	24
4.2.2. <i>Une prolifération de projets de vidéosurveillance dans les lieux publics</i> .....	25
4.2.3. <i>Des analyses préalables à l'installation de la vidéosurveillance insatisfaisantes</i> .....	26
4.2.4. <i>Des interventions qui dépassent l'expertise de la CAI</i> .....	27
4.2.5. <i>Une efficacité difficile à mesurer de façon précise</i> .....	28
4.2.6. <i>Une implication élargie pouvant enrichir la réflexion</i> .....	29
4.2.7. <i>Une politique écrite mieux encadrée</i> .....	29
4.2.8. <i>Un suivi irrégulier et un encadrement insuffisant des projets de vidéosurveillance</i> ..	30
<b>5. COMPÉTENCE, POUVOIRS, STRUCTURE ET FONCTIONS</b> .....	<b>33</b>
5.1. ENTRE COMPÉTENCE, POUVOIRS ET FONCTIONS .....	33
5.2. LA STRUCTURE DE LA CAI ET SA DOUBLE FONCTION .....	34
5.3. LA RÉPARTITION DE LA COMPÉTENCE EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS ENTRE LES ORGANISMES PUBLICS ET LA CAI.....	36
5.3.1. <i>Les organismes publics et la protection des renseignements personnels</i> .....	36
5.3.2. <i>Le rôle de surveillance et de contrôle de la CAI</i> .....	39
<b>6. LES POUVOIRS DE LA CAI POUR EXERCER SON RÔLE DE SURVEILLANCE</b> .....	<b>40</b>
6.1. LES POUVOIRS SPÉCIFIQUES DE LA COMMISSION.....	40
6.1.1. <i>Approbation préalable ou avis favorable de la Commission au sujet d'une entente de communication entre organismes</i> .....	40
6.1.2. <i>Transmission d'une entente ou information préalable à la Commission</i> .....	41
6.1.3. <i>Exiger la tenue et l'inscription dans un registre</i> .....	41
6.1.4. <i>Obligation pour un organisme public d'adopter des directives</i> .....	42
6.1.5. <i>La CAI peut-elle exercer ses pouvoirs comme si elle exigeait une autorisation préalable à la vidéosurveillance?</i> .....	42

6.1.6. <i>La Commission dispose-t-elle d'un pouvoir réglementaire ou de directive générale en matière de vidéosurveillance?</i> .....	43
6.2. LES POUVOIRS GÉNÉRAUX DE LA CAI .....	46
6.2.1. <i>Pouvoir d'enquête et d'inspection</i> .....	46
6.2.2. <i>Pouvoir d'ordonnance</i> .....	47
6.2.3. <i>Pouvoir de saisir le gouvernement</i> .....	47
6.2.4. <i>Prescrire des conditions applicables à un fichier de renseignements personnels</i> ....	47
6.2.5. <i>Comment peuvent être utilisés les pouvoirs généraux de la CAI en matière de vidéosurveillance?</i> .....	48
<b>7. ANALYSE DES RÈGLES D'UTILISATION DE LA VIDÉOSURVEILLANCE</b> .....	<b>50</b>
7.1. STATUT JURIDIQUE DES RÈGLES.....	50
7.2. BRÈVE ANALYSE SUR LE FOND DES VINGT RÈGLES .....	52
7.2.1. <i>Les principes de la nécessité, de la finalité et de la proportionnalité et les règles 1, 2, 3, 4, 5, 8, 10, 11, 12, 13, 18 et 20</i> .....	52
7.2.2. <i>Les principes de la légitimité et de la transparence et les règles 6, 7, 9, 15 et 19</i> ....	55
7.2.3. <i>Les principes de confidentialité et de sécurité et les règles 14, 16 et 17</i> .....	57
7.3 CONCLUSION DE L'ANALYSE JURIDIQUE DES RÈGLES D'UTILISATION DE LA VIDÉOSURVEILLANCE .....	59
7.3.1. <i>Les règles qui reprennent autrement ce que dit déjà la loi</i> .....	60
7.3.2. <i>Les règles qui devraient être édictées par voie réglementaire et qui sont donc ultra vires des pouvoirs de la CAI</i> .....	60
7.3.3. <i>Les règles qui contredisent une disposition de la LAI</i> .....	62
<b>8. LE POUVOIR RÉGLEMENTAIRE DU GOUVERNEMENT QUANT AUX MESURES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS</b> .....	<b>63</b>
8.1. LE RÈGLEMENT SUR LA DIFFUSION DE L'INFORMATION ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS .....	63
8.1.1. <i>Champ d'application du Règlement</i> .....	63
8.1.2. <i>Encadrement de la vidéosurveillance selon le Règlement r. 0.2</i> .....	65
8.1.3. <i>Observations générales sur le Règlement r. 0.2</i> .....	66
8.1.4. <i>Suggestion pour une meilleure évaluation du règlement r.0.2</i> .....	68
8.2. LA PARTICIPATION DE LA CAI À LA RÉFLEXION MENANT À LA PRÉPARATION D'UN NOUVEAU RÈGLEMENT .....	69
<b>9. CONCLUSION</b> .....	<b>71</b>

---

## 1. Sommaire

La Commission d'accès à l'information du Québec nous a confié le mandat de réviser le document de la Commission, intitulé *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, publié en juin 2004. Nous concluons que cette voie n'offre aucune solution aux embûches que rencontre la Commission et qu'il faut plutôt orienter l'action de la Commission vers une autre stratégie.

La Commission fait face à des difficultés à faire respecter ces vingt règles auprès des organismes publics, et notamment auprès des corps policiers. Les obstacles tiennent autant à la résistance qu'opposent les corps policiers et les municipalités qu'au caractère souvent vague et difficilement opérationnel des règles. La Commission est préoccupée par le déploiement de la vidéosurveillance dans les lieux publics et s'interroge sur la meilleure façon d'y faire face, en posant l'hypothèse que la révision des Règles permettrait de renouveler sa méthode et d'accroître l'efficacité de ses pouvoirs de contrôle et de surveillance.

Une analyse des guides adoptés par les autres provinces canadiennes et le gouvernement fédéral nous a d'abord permis de constater que le contenu des règles est assez similaire d'une province à l'autre, le Québec se distinguant non pas par le type de règles, mais plutôt par le caractère souvent plus général des prescriptions. Bref, l'orientation des règles semble assez bien partagée par l'ensemble des autres provinces canadiennes, confirmant ainsi le caractère approprié du type de règles que tentent de mettre en œuvre tous les commissaires à la vie privée à travers le pays.

L'analyse de la démarche suivie par la Commission lors de ses enquêtes pratiquées entre 1992 et 2006 sur des projets de vidéosurveillance de trois centre-villes du Québec (Sherbrooke, Baie-Comeau et Montréal) démontre que l'élaboration de règles plus détaillées, qui sont passées de dix à vingt au fil des ans, n'a pas pour autant facilité le travail des enquêteurs de la Commission. En effet, pendant que la Commission a cessé tout suivi des projets de Sherbrooke et de Baie-Comeau, elle n'a jamais réussi à finaliser son rapport au sujet de la vidéosurveillance du centre-ville de Montréal par le SPVM. Une analyse des échanges documentaires entre la CAI et les municipalités ou corps policier en cause a permis de constater que la Commission exerce ses pouvoirs de façon à requérir l'équivalent d'une autorisation préalable à l'implantation ou l'élargissement de la vidéosurveillance, tout en procédant à une investigation poussée des analyses faites par les municipalités ou corps policiers, remettant en question la justification du recours à la vidéosurveillance pour combattre le crime et les infractions à la loi.

Il fallait donc trouver la cause profonde du malaise qui oppose la CAI et les responsables de ces projets, notamment lorsque la Commission tente d'établir ses

---

exigences concernant la démonstration du principe de nécessité, préoccupée à juste titre qu'est la Commission de l'impact inédit de l'utilisation de cette technologie sur la vie privée des centaines de milliers de passants qui circulent dans les aires vidéosurveillées.

Une analyse détaillée des compétences, pouvoirs et fonctions de la Commission nous a permis de faire certaines observations. La Commission exerce une compétence en matière de protection des renseignements personnels, par laquelle elle doit surveiller le respect par les organismes publics des principes inscrits à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. La Commission se divise en deux sections, chacune responsable d'assurer le respect de la loi. Une première section juridictionnelle entend, à l'exclusion de tout autre tribunal, toute demande de révision faite en vertu de la loi, pendant que la section de surveillance doit vérifier le respect des normes de protection des renseignements personnels par les organismes publics. Certains amendements à la loi de 2006 ont ajouté certains verrous afin de diminuer la crainte de partialité de la CAI en raison de ce cumul de fonction. Il ne faut par contre pas oublier que la règle de l'impartialité de la CAI doit également prévaloir au sein de chacune de ses sections. Or, la Commission se place dans une situation attaquable lorsqu'elle se charge d'appliquer des règles qu'elle a elle-même développé et adopté et, qu'en outre, elle exerce par l'adoption de ces règles un pouvoir réglementaire qui ne lui appartient pas.

Les principes de protection des renseignements personnels de la loi peuvent se résumer par les principes de la confidentialité, de la sécurité, de la nécessité et proportionnalité, de la transparence et de la finalité. Ces principes sont énoncés de façon très large dans la loi, sans que des règlements permettent d'en préciser la nature et le caractère opérationnel.

La loi attribue à la Commission certains pouvoirs pour s'acquitter de sa compétence de surveillance. On peut distinguer les pouvoirs spécifiques des pouvoirs généraux d'enquête et d'ordonnance. Les pouvoirs spécifiques offrent certains outils, comme l'autorisation préalable que doivent obtenir de la Commission les organismes qui voudraient faire certaines manipulations de renseignements personnels, précisées dans la loi. Aucune de ces situations prévues à la loi ne s'applique à la vidéosurveillance, à moins que les renseignements ne soient transmis à un autre organisme public. Quant aux pouvoirs généraux d'enquête de la Commission, l'expérience de l'enquête menée par la CAI au sujet des trois systèmes de vidéosurveillance, démontre qu'ils ne permettent pas de conclure à des mécanismes favorables à une meilleure gestion et contrôle de la vidéosurveillance.

Il faut donc revenir au statut juridique des vingt Règles étudiées, surtout depuis l'entrée en vigueur de l'article 63.2 de la loi le 15 juin 2007. Cette disposition confère en exclusivité au gouvernement du Québec le pouvoir d'adopter des règlements pour

---

édicter les mesures qui doivent être prises pour assurer le respect des principes de protection des renseignements personnels inscrits à la loi. La Commission ne peut dès lors plus se substituer au silence de la loi pour édicter des mesures qui relèvent du pouvoir réglementaire inscrit à la loi.

L'analyse plus détaillée des vingt règles nous permet d'identifier trois catégories de règles. Une première catégorie est composée de règles qui sont plus ou moins des paraphrases des principes énoncés à la loi. Si leur validité juridique ne fait pas de doute, leur utilité pour les inspecteurs de la commission à qui on demande d'en assurer leur respect est discutable puisqu'elles n'offrent aucune norme d'application opérationnelle. De plus, leur caractère vague peut donner lieu à des applications plus ou moins poussées, selon les dossiers.

La deuxième catégorie de règles se compose de normes qui relèvent du pouvoir réglementaire de la loi, confié au gouvernement, en édictant des mesures de protection au sens où le prévoit l'article 63.2 de la loi. Ces règles seraient donc invalides ou non opposables aux organismes publics, puisque seul un règlement dûment adopté en vertu de la loi pourrait imposer ce type de mesures aux organismes publics. De plus, une simple directive administrative ne saurait limiter l'étendue du pouvoir discrétionnaire confié par la loi aux organismes comme les corps policiers ou les municipalités qui disposent de compétences propres en matière de maintien de la paix et de sécurité civile.

Une troisième catégorie, enfin, regroupe des règles qui pourraient contredire ou contrevir à l'article 65 de la loi, du moins lorsqu'elles sont opposées aux corps policiers, puisque cet article prévoit que le principe de transparence qui y est inscrit ne s'applique pas aux organismes chargés de prévenir ou réprimer le crime.

La voie réglementaire apparaît dès lors comme la seule véritable issue pour résoudre les difficultés que rencontre la Commission pour mieux faire respecter les principes de la loi en matière de protection des renseignements personnels lors de la vidéosurveillance. Un Règlement a déjà été adopté en 2008 où on trouve une première tentative d'incorporer dans des normes l'encadrement de la vidéosurveillance.

Ce règlement ne s'applique pas aux organismes publics décentralisés, comme les organismes municipaux, scolaires et sociosanitaires. On peut noter par ailleurs qu'il ajoute relativement peu de clarifications concernant les mesures de protection qui doivent être mises en place, au-delà de la nécessité de préciser ces mesures, par le biais d'un comité interne.

Il serait dès lors important de vérifier si cette méthode avancée par le règlement réussi à induire une plus grande responsabilisation des ministères (notamment Transports

---

Québec) qui y sont déjà assujettis et ont déjà lancé des projets de vidéosurveillance, face à leurs responsabilités en matière de protection des renseignements personnels.

Nous suggérons qu'une analyse de l'impact du Règlement sur des projets en cours soit entamée rapidement, en collaboration avec la Direction de l'accès à l'information et de la protection des renseignements personnels (DAIPRP) du Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information (SRIDAI). On sait que cette direction prépare déjà un autre Règlement avec comme hypothèse de discussion une méthode similaire, pour assujettir les organismes publics décentralisés, dont les organismes municipaux.

Afin d'assurer un meilleur respect des droits des citoyens en matière de vidéosurveillance par les organismes publics responsables en premier lieu du respect de ces principes, d'une part, et une meilleure utilisation des fonctions et pouvoirs de surveillance et de contrôle que la loi confie à la CAI, la Commission devrait être associée au plus tôt à la démarche de préparation d'un nouveau règlement, pour que son expertise soit mise à contribution, et ce, dans le meilleur intérêt de tous.

---

## 2. Introduction

La Commission d'accès à l'information du Québec [ci-après CAI] a confié à deux professeurs-chercheurs de l'ENAP, Christian Boudreau et Marie-Claude Prémont, le mandat de revoir le document de la Commission, intitulé *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, publié en juin 2004.

De l'avis de la CAI, la gestion récente des dossiers de vidéosurveillance suscite des questions importantes de la part de certains organismes publics soumis aux pouvoirs de surveillance de la Commission, en plus de soulever des interrogations au sein même de la Commission quant à la conformité et à la pertinence de l'étendue de l'exercice des pouvoirs et des compétences de la Commission sur certains dossiers contentieux.

La réflexion dans laquelle est engagée la Commission s'illustre sans doute par le dossier toujours en suspens de l'avis final quant à l'utilisation des caméras de surveillance par le Service de police de la ville de Montréal sur la rue St-Denis à l'été 2005 pour prévenir la vente de drogues illicites et d'actes de vandalisme sur la propriété environnante. Entre-temps, les caméras de vidéosurveillance semblent être installées en permanence dans différents projets alors que leur utilisation se banalise jusque dans les transports en commun, visant quotidiennement des centaines de milliers d'usagers.

Le principal motif avancé pour l'installation de caméras de vidéosurveillance dans les lieux publics par les organismes publics concerne la sécurité publique, sous toutes ses formes<sup>1</sup>. Les systèmes de vidéosurveillance viseraient ainsi la prévention et la répression d'actes criminels ou d'infractions à la loi, notamment la vente de drogues illicites, les voies de fait sur les personnes, y compris sur des employés qui fournissent des services publics, les actes de vandalismes contre la propriété publique ou privée, pour nommer les situations les plus fréquentes.

La CAI se demande où commence et où s'arrête sa compétence en matière de vidéosurveillance quant au contrôle qu'elle doit exercer sur les organismes publics qui en font usage, et particulièrement face aux corps policiers à qui est confiée la mission de prévention du crime et de respect de la loi. Jusqu'à quel point la Commission peut-elle réviser et contrôler l'analyse que font les corps policiers de la pertinence et de la nécessité de recourir à des mécanismes de vidéosurveillance pour prévenir et réprimer

---

<sup>1</sup> Sur le concept de société du risque et le rôle des nouvelles technologies de surveillance, on consultera : Commission de l'éthique de la science et de la technologie, *Viser un juste équilibre. Un regard éthique sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité*. Avis, Gouvernement du Québec, 2008, 67 p. plus les annexes.

---

le crime? La CAI se demande quelles sont les mesures ou les mécanismes à mettre en place pour s'assurer que les organismes publics assument correctement leurs responsabilités quant à l'utilisation des caméras de vidéosurveillance dans le respect des principes qui garantissent la vie privée et la protection des renseignements personnels.

Afin de remplir le mandat qui nous est confié par la CAI, nous proposons de procéder en six étapes. Nous ferons d'abord une analyse comparative des règles d'utilisation de la vidéosurveillance dans les autres provinces canadiennes (section 0), avant de jeter un regard analytique sur la démarche suivie jusqu'ici par la CAI dans trois dossiers de vidéosurveillance sur lesquels elle s'est prononcée (section 0). Par la suite, nous présenterons une analyse de la structure, des compétences (section 5) et des pouvoirs de la CAI en matière de protection des renseignements personnels et vidéosurveillance<sup>2</sup>, en distinguant les pouvoirs spécifiques de la CAI de ses pouvoirs généraux (section 6). Cette analyse nous permettra par la suite de mieux caractériser chacune des vingt règles de la CAI, sur le plan de leur valeur juridique (section 7). Nous poursuivrons par la suite en analysant le règlement adopté en 2008 par le gouvernement, afin de donner quelques indications quant à la gestation actuelle d'un nouveau règlement pour assujettir les organismes publics décentralisés (section 8), avant de conclure (section 0).

---

<sup>2</sup> *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1 [ci-après LAI, pour Loi d'accès à l'information].

---

### 3. Analyse comparée des guides d'utilisation de la vidéosurveillance dans les lieux publics au Canada

Des règles régissant l'utilisation de la vidéosurveillance dans les lieux publics ont été proposées pour la première fois au Canada dans un rapport d'investigation, rendu public le 31 mars 1998, par le commissaire à la vie privée de la Colombie-Britannique, David H. Flaherty. Ce document allait servir de modèle pour les autres commissaires provinciaux afin d'élaborer leurs propres règles en matière de vidéosurveillance. Une majorité de provinces disposent aujourd'hui de telles règles, adoptées et révisées selon l'ordre chronologique suivant :

- Colombie-Britannique : adoption : 21 juin 2000; révision : 26 janvier 2001.
- Ontario : adoption : octobre 2001; révision : septembre 2007.
- Québec : adoption : 3 mai 2002; révision : juin 2004<sup>3</sup>.
- Alberta : adoption : juin 2004.
- Saskatchewan : adoption : 24 juin 2004.
- Nouveau-Brunswick : publication dans le rapport annuel de 2004-2005.
- Terre-Neuve : adoption : mai 2005.
- Nouvelle-Écosse : publication dans le rapport annuel de 2006.

Le commissaire à la protection de la vie privée du Canada a, à son tour, émis des règles concernant l'utilisation de la vidéosurveillance par les organismes fédéraux dans les lieux publics, en mars 2006.

La CAI présente les règles en disant qu'elles « ont pour but d'encadrer les prises de décisions des organismes publics en leur proposant une démarche qui leur permettra de trouver un juste équilibre entre la protection des renseignements personnels, la vie privée et la sécurité »<sup>4</sup>. Ces règles ne s'appliquent pas à la surveillance comme outil d'enquête utilisé dans les cas où la loi ou un mandat de perquisition l'autorise. Elles ne visent pas non plus la surveillance des lieux de travail des employés, ni les lieux privés comme les chambres d'hôpitaux ou les salles d'essayage.

Dans le texte, nous utilisons le terme *guide* pour désigner les documents produits par les commissaires provinciaux et canadien concernant les règles d'utilisation de la vidéosurveillance dans les lieux publics par les organismes publics. Afin de comparer les guides entre eux, nous avons d'abord dressé une liste d'énoncés qui couvrent l'ensemble des règles présentes dans les guides (voir tableau 1).

---

<sup>3</sup> Une consultation publique menée par la CAI en septembre 2003 conduit à l'adoption, en juin 2004, d'une nouvelle série de règles d'utilisation de la vidéosurveillance dans les lieux publics : le nombre de règles sur la vidéosurveillance passe alors de 10 à 20.

<sup>4</sup> Commission d'accès à l'information (2004), *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, p. 1.



Nous avons ensuite regroupé ces énoncés autour des thèmes généraux suivants : la nécessité et la proportionnalité, la gestion des images filmées et des enregistrements, la légitimité et la responsabilité, l'évaluation et la vérification périodiques ainsi que la démarche et la transparence.

<b>Tableau 1 : Règles d'utilisation de la vidéosurveillance adoptées par les commissaires à la protection de la vie privée de provinces canadiennes</b>											
	Qc 2002	Qc 2004	Alb 2001	Ont 2001	NB 2004	TN 2005	NÉ 2006	SK 2004	CB 1998	CB 2001	Can 2006
<b>La nécessité et la proportionnalité</b>											
• S'assurer que le problème à régler est sérieux		X			X		X				X
• Documenter et circonscrire le problème à régler	X	X	X	X	X	X	X	X	X	X	X
• Empêcher détournement de finalités		X		X	X		X		X		X
• Limiter l'utilisation des caméras à des périodes, des lieux ou des événements où c'est nécessaire	X	X	X	X	X	X	X	X	X	X	X
• Ne pas permettre de filmer certains lieux plus privés (fenêtres, toilettes, salle d'essayage, etc.)	X	X	X	X	X	X		X	X	X	X
• Évaluer l'impact des caméras sur la vie privée	X	X	X	X	X	X	X	X		X	X
• Envisager, évaluer ou mettre à l'essai des mesures moins intrusives au regard de la vie privée.	X	X	X	X	X					X	X
• Démontrer que les bénéfices sont supérieurs aux atteintes à la vie privée		X	X	X	X	X		X		X	X
<b>La gestion des images et des enregistrements</b>											
• Si possible, n'enregistrer que lorsque la situation l'exige	X	X	X			X	X	X			X
• Fixer une durée de conservation des enregistrements	X	X	X	X	X		X		X	X	X
• Prévoir des mécanismes de destruction d'enregistrements			X	X	X	X		X	X	X	
• Préciser les circonstances justifiant ou interdisant l'accès aux enregistrements et les personnes autorisées		X	X	X	X	X		X	X	X	X
• Prévoir des mesures de sécurité afin de restreindre l'accès aux seules personnes autorisées	X	X	X	X	X	X		X	X	X	
• Prévoir un registre d'inscription des accès			X	X	X	X		X	X		
• Cacher ou positionner les écrans de visionnement de manière à ce que le public ne les voit pas			X	X	X	X		X	X	X	
• Permettre accès aux enregistrements par personnes filmées	X	X	X	X	X	X		X	X	X	X
<b>La légitimité et la responsabilité</b>											
• S'assurer de la légitimité/légalité de l'organisme à collecter et détenir des renseignements personnels					X	X		X		X	X
• Se donner une politique écrite		X	X	X	X	X	X	X	X	X	X
• Nommer une personne responsable		X	X	X	X	X	X	X		X	X
• (In)former les différents intervenants	X	X	X	X	X				X	X	
• Signer des ententes avec le personnel et les fournisseurs qui précisent leurs responsabilités			X	X	X	X	X			X	
• Prévoir des sanctions			X	X	X	X	X	X		X	X
• Réviser et mettre à jour régulièrement la politique			X	X	X	X		X		X	
<b>L'évaluation et la vérification (audit) périodiques</b>											
• Évaluer la nécessité de poursuivre la vidéosurveillance	X	X		X	X	X		X		X	X
• Vérifier la conformité des conduites à la politique écrite			X	X	X	X		X	X	X	X
• Vérificateur/évaluateur externe				X	X						X
<b>La démarche et la transparence</b>											
• Consulter les parties prenantes		X	X	X	X	X		X		X	X
• Afficher présence des caméras et responsables à contacter	X	X	X	X	X	X		X	X	X	X
• Rendre publics les résultats de l'évaluation					X	X		X			X
<b>Varia</b>											
• Interdire interconnexion, couplage et biométrie		X									

---

### **3.1. La nécessité et la proportionnalité**

La majorité des guides conviennent de l'importance de bien documenter le problème à résoudre avec des données probantes afin de s'assurer qu'il est réel, circonscrit et sérieux. Les caméras doivent s'attaquer à des problèmes précis et importants (ex : crimes contre la personne ou la propriété). Bien que dérangeants, les incivilités et les comportements déviants (itinérance, consommation d'alcool, prostitution) ne doivent pas justifier l'installation de caméras. Pour l'ensemble des guides, l'utilisation des caméras doit aussi être circonscrite de manière à tenir compte des périodes où se produisent habituellement les crimes. De plus, les caméras ne doivent pas être dirigées vers des endroits où les gens s'attendent à préserver leur intimité, comme les fenêtres d'immeubles, les salles d'essayage et les toilettes. Les techniques de masquage peuvent s'avérer utiles dans ce cas-ci pour que la vidéosurveillance ne déborde pas vers ce type d'espace. Les organismes publics doivent s'assurer que les caméras ne servent qu'à des fins légitimes (ex : sécurité publique) et éviter qu'il y ait détournement de finalité (ex : profilage racial).

Tous les guides soulignent l'importance d'évaluer l'impact des caméras sur la vie privée. À cet égard, les commissaires de l'Alberta<sup>5</sup> et de la Colombie-Britannique<sup>6</sup> mettent à la disposition des organismes publics des documents qui, sous forme de questionnaire, les guident dans la réalisation des évaluations d'impact.<sup>7</sup>

L'organisme public doit faire la démonstration que la vidéosurveillance procure des bénéfices supérieurs aux atteintes à la vie privée et que d'autres mesures moins intrusives ont été envisagées ou mises à l'essai. La vidéosurveillance doit être vue comme une mesure exceptionnelle et de dernier recours.

### **3.2. La gestion des images et des enregistrements**

Les règles de gestion des images et des enregistrements proposées par les guides visent à restreindre le recours et l'accès aux images, ainsi que la durée de conservation des enregistrements. Lorsqu'un opérateur examine les images filmées, on recommande habituellement que celui-ci attende d'avoir des motifs de croire qu'une infraction sera

---

<sup>5</sup> <http://www.oipc.ab.ca/ims/client/upload/pia-instructions-1.1.pdf>

<sup>6</sup> [http://www.oipcbc.org/sector\\_public/resources/pia.htm](http://www.oipcbc.org/sector_public/resources/pia.htm)

<sup>7</sup> Ces documents ne s'adressent pas seulement à des projets de vidéosurveillance, mais à tout nouveau projet ou programme mis en œuvre par un organisme public dont la gestion des renseignements personnels peut avoir un impact sur la vie privée.

---

commise avant de démarrer l'enregistrement. On recommande également de détruire les enregistrements lorsqu'ils ne sont plus nécessaires.

En l'absence d'infractions, les guides suggèrent des durées de conservation qui varient de 24 heures à 21 jours.

Le guide du Québec, quant à lui, ne suggère aucune durée de conservation. Si un incident se produit, on reconnaît que ce délai peut être prolongé, le temps de faire la lumière sur l'événement et, au besoin, de procéder à l'enquête et aux poursuites judiciaires.

Les guides ne précisent pas si un mandat est nécessaire pour accéder aux enregistrements. Tous les guides signalent l'importance de mettre en place des mesures de sécurité qui permettent de contrôler l'accès aux écrans de visionnement et aux enregistrements des images. À ce propos, plusieurs guides s'avèrent plus précis que celui du Québec, notamment en ce qui concerne l'emplacement et le positionnement des écrans de visionnement ou la création d'un registre d'accès aux enregistrements.

### **3.3. La légitimité et la responsabilité**

Plusieurs guides soulignent que les organismes publics qui procèdent à une installation de caméras de vidéosurveillance doivent s'assurer de la légitimité et de la compétence légale à le faire. Tous les guides recommandent aux organismes de se doter d'une politique écrite au sujet de la vidéosurveillance. Cette politique peut contenir les modalités de fonctionnement des caméras, les conditions d'accès et de conservation des enregistrements, les rôles et responsabilités des organismes et des intervenants, les mesures de révision et les sanctions.

Alors que la majorité des guides donnent des précisions sur ce que devrait contenir une telle politique, le guide du Québec n'en donne aucune, sinon que « cette politique devrait notamment définir le mécanisme de consultation du public avant de procéder à l'utilisation de la vidéosurveillance ».

### **3.4. L'évaluation et la vérification périodiques**

Les guides précisent que l'installation de caméras de vidéosurveillance ne peut constituer une solution fixe et permanente. La vidéosurveillance doit être vue comme un projet en constante évaluation et non comme une infrastructure permanente. La majorité des guides suggèrent d'ailleurs d'évaluer à chaque année la nécessité de poursuivre la vidéosurveillance. Le problème persiste-t-il? Les caméras sont-elles encore le meilleur moyen pour y remédier? Doit-on ajuster certaines modalités? Presque tous les guides, à

---

l'exception de celui du Québec, recommandent de procéder à des vérifications périodiques (*audit*) afin de s'assurer que les différents intervenants respectent la politique d'utilisation de la vidéosurveillance que s'est donné l'organisme public. Par exemple, utilise-t-on correctement le système de caméras et que fait-on avec l'information recueillie? Certains guides recommandent que l'évaluation, tout comme la vérification, se fassent par des agents externes à l'organisme responsable des caméras.

### **3.5. La démarche et la transparence**

Tous les guides suggèrent qu'il y ait consultation auprès des populations concernées avant d'installer des caméras. De plus, des affiches visibles doivent annoncer de manière claire que l'endroit fait l'objet de vidéosurveillance. Ces avis doivent aussi indiquer le nom et le numéro de la personne responsable à contacter, notamment si une personne a des questions ou des plaintes à formuler ou si elle veut exercer son droit d'accès aux images qui la concernent. Certains guides suggèrent aussi de rendre publics les résultats des évaluations ou des vérifications.

### **3.6. Sommaire de l'analyse comparative des guides du Canada**

L'examen des guides fait ressortir l'importance des principes de nécessité, de proportionnalité, de sécurité, de responsabilité, de légitimité et de transparence dans l'encadrement de la vidéosurveillance. Cette analyse comparée montre qu'il y a convergence dans les règles d'utilisation de la vidéosurveillance adoptées par les commissaires provinciaux ainsi que par le commissaire canadien. Le guide du Québec semble s'inscrire dans cette mouvance pancanadienne lorsqu'il s'agit d'encadrer la vidéosurveillance dans les lieux publics. S'il y a des différences entre le guide du Québec et les autres guides, elles se situent non pas tant dans l'énoncé des règles que dans leur degré de précision et d'opérationnalisation. C'est le cas des règles relatives à la sécurité et à la responsabilité.

Alors que plusieurs guides précisent les mesures de sécurité à mettre en place pour protéger et contrôler l'accès aux visionnements et aux enregistrements ainsi que les éléments que doivent couvrir la politique écrite de l'organisme responsable, le guide du Québec ne donne presque aucune indication à cet égard. Certains guides proposent aussi un questionnaire permettant de réaliser l'évaluation d'impact des mesures de surveillance sur la vie privée. La comparaison des guides provinciaux soulève la question suivante : ne serait-il pas plus aidant pour les organismes publics du Québec de disposer de plus d'indications pour la mise en place de mesures de sécurité, l'élaboration de leur politique et pour l'évaluation des impacts sur la vie privée?

---

Nous allons maintenant examiner l'application des règles d'utilisation de la vidéosurveillance par des organismes publics québécois dans trois projets et l'évaluation qu'en a proposée la CAI.

---

## 4. Examen de trois projets de vidéosurveillance ayant fait l'objet d'enquête par la CAI

La prolifération de la vidéosurveillance dans les lieux publics préoccupe la CAI depuis plusieurs années. Trois projets de vidéosurveillance ont plus particulièrement attiré l'attention de la CAI au point de l'amener à faire enquête. Dans les trois cas, il s'agit de rues commerciales situées dans des centres-villes. Les villes en question sont Sherbrooke, Baie-Comeau et Montréal. L'analyse de la documentation<sup>8</sup> entourant ces trois projets permet de faire certains constats quant au respect des règles d'utilisation de la vidéosurveillance par les organismes publics ainsi que sur la façon dont la CAI est intervenue, notamment lors de ses enquêtes.

### 4.1. Description sommaire des projets et de la surveillance exercée par la CAI

#### 4.1.1. CENTRE-VILLE DE SHERBROOKE

La ville de Sherbrooke décide en 1990 de sécuriser le centre-ville en installant quatre caméras de vidéosurveillance sur la rue Wellington sud. Il s'agit d'une des premières villes canadiennes à installer des caméras dans ses rues afin de combattre la criminalité qui y sévit. Ces caméras enregistrent sur ruban vidéo des images en continu, lesquelles sont conservées pendant une semaine avant d'être effacées. La ville installe en avril 1992 une cinquième caméra pour surveiller le stationnement à l'entrée de l'hôtel de ville. Les écrans, qui donnent accès aux images captées, sont installés dans un centre d'urgence 911. Le personnel du centre, dont les tâches consistent avant tout à répondre au téléphone, surveille en même temps les écrans et contacte la police au moment d'incidents.

S'interrogeant sur la légalité et le caractère intrusif de l'enregistrement des images captées par caméras, la *Ligue des droits et libertés* porte plainte à la CAI. Celle-ci décide alors d'aller enquêter sur le terrain le 28 avril 1992. Tout en soutenant que la criminalité a chuté de 22 % depuis l'installation des caméras de vidéosurveillance, « [l]e Service de police de la ville de Sherbrooke reconnaît qu'en deux ans, il n'a visionné les bandes vidéo qu'une fois ou deux afin de faire progresser l'enquête relative à certains délits »<sup>9</sup>. La CAI en déduit que la seule présence de caméras, et non l'enregistrement des images, constitue l'élément dissuasif. Si la CAI reconnaît que la surveillance par

---

<sup>8</sup> Essentiellement des rapports d'enquêtes, des rapports d'évaluation et des articles de journaux.

<sup>9</sup> Commission d'accès à l'information (1992), *Rapport final d'enquête. La Ville de Sherbrooke*, p. 7.

---

caméra sans enregistrement ne contrevient pas à la LAI et qu'elle contribue à la réduction de la criminalité, elle conclut que « l'enregistrement [continu] des images n'est pas nécessaire parce qu'il n'apporte rien de plus à la protection du public que la présence des caméras n'assure déjà »<sup>10</sup>.

La Ville de Sherbrooke cesse alors l'enregistrement continu des images captées par les caméras à partir du 22 octobre 1992, mais elle autorise le personnel du centre 911 à enregistrer lorsqu'un crime est en train de se commettre ou sur le point de l'être et d'en aviser les policiers. Jusqu'en 2003, la Ville poursuit le déploiement de caméras dans son centre-ville. On en dénombre alors seize, dont quatre sont situées dans des parcs près du centre-ville. Lors de la consultation publique menée en septembre 2003 par la CAI, la Ville présente un mémoire dans lequel elle préconise un assouplissement des règles d'enregistrement et annonce qu'elle étudie la possibilité d'enregistrer de façon continue les images captées dans certains lieux jugés problématiques. Elle y soutient aussi que le meurtre de Julie Boisvenu, survenu en juin 2002, aurait peut-être été évité si les caméras de vidéosurveillance avaient enregistré le soir de son enlèvement sur une rue adjacente à la rue Wellington.

Les enregistrements auraient tout au moins « permis d'identifier et de retrouver plus rapidement l'agresseur »<sup>11</sup>. La Ville poursuit le déploiement des caméras dans le centre-ville.

En mai 2004, le comité exécutif de la Ville de Sherbrooke approuve la mise sur pied d'un projet pilote d'enregistrement continu qui s'étend sur neuf semaines, du 23 juin au 21 août 2004. Pendant ce projet, un étudiant surveille les images des caméras en opération afin de « documenter le besoin et l'utilité de nos caméras actuelles; constater si l'assignation d'une ressource dédiée exclusivement à cette tâche augmentait l'efficacité de celle-ci; évaluer une technologie permettant la surveillance de plusieurs caméras simultanément par une seule personne ». <sup>12</sup>. En mai 2005, le comité de sécurité de la Ville décide de ne pas reconduire le projet pilote et de cesser l'enregistrement continu.

Selon ce comité, « la Ville ne peut démontrer par son projet pilote qu'elle est aux prises avec un problème de criminalité suffisamment documenté pour faire autoriser un enregistrement en continu ... un objectif de prévention générale du crime n'est pas suffisant pour justifier l'enregistrement des images ». <sup>13</sup> Les règles émises par la CAI, en

---

<sup>10</sup> *Ibid.* p. 8.

<sup>11</sup> Ville de Sherbrooke, courriel envoyé à la Commission d'accès à l'information le 8 septembre 2003, [http://ville.sherbrooke.qc.ca/fr/conseil/memoire\\_01.html](http://ville.sherbrooke.qc.ca/fr/conseil/memoire_01.html)

<sup>12</sup> Ville de Sherbrooke, Communiqué du 12 mai 2005, *Caméras de surveillance*, p. 2.

<sup>13</sup> *Idem.*

---

2004, rendent plus difficile la justification de la vidéosurveillance par la Ville, précise ce comité.

Pierre-Hugues Boisvenu, le père de Julie Boisvenu assassinée trois ans plus tôt, dénonce cette décision et organise une marche dans les rues de Sherbrooke qui attire plus de 200 personnes. Face à cette manifestation en faveur de l'enregistrement et en réponse aux nombreuses interventions de Pierre-Hugues Boisvenu dans les différents médias, la Ville décide de poursuivre le projet pilote à l'été 2005. Celui-ci se déroule du 16 juin au 25 septembre. La CAI décide de mener une nouvelle enquête à l'automne 2005. Elle réalise alors une analyse préliminaire, laquelle constitue la dernière intervention de la CAI dans ce dossier.

Entre-temps, le projet d'enregistrement des images captées par les caméras de vidéosurveillance reprend chaque été. Les images enregistrées seraient conservées pendant 7 jours. Selon les élus municipaux, il ne s'agirait plus d'un projet pilote, mais d'un programme bien établi.<sup>14</sup>

#### 4.1.2. CENTRE-VILLE DE BAIE-COMEAU

La Ville de Baie-Comeau décide en mars 2002 d'installer deux caméras de vidéosurveillance au centre-ville, secteur de Mingan. Cette décision fait suite à une demande des commerçants du secteur de Mingan qui se montrent inquiets face à l'augmentation de la criminalité, en particulier des incendies dans des conteneurs à ordures du centre-ville.

On craint alors que « les incendies répétitifs dans les conteneurs se propagent aux édifices voisins et qu'une conflagration majeure survienne dans ce secteur commercial »<sup>15</sup>. Ces caméras visent à dissuader et à prévenir de tels incidents plutôt qu'à prendre les délinquants ou criminels sur le fait et à faire enquête. La Ville installe, le 3 mai 2002, une caméra de vidéosurveillance au coin des rues Jalbert et De Puyjalon, et une deuxième en octobre 2002. Les caméras opèrent 24 heures par jour. Les images captées sont détruites après 26 heures, à moins qu'une dénonciation d'acte criminel ne soit faite auprès de la Sûreté du Québec. Le visionnement des images captées se fait dans les locaux de Centralarme, une entreprise privée qui a pour mandat de répondre aux appels 911. Les préposés de Centralarme n'ont pas accès aux images enregistrées. « Les policiers et les enquêteurs en sinistre qui veulent y avoir accès doivent

---

<sup>14</sup> Rita Legault, *Sherbrooke Record*, 20 juin 2008, "You're on candid camera: Downtown video taping a fact of life".

<sup>15</sup> Ville de Baie-Comeau (2003), *Rapport du Comité de concertation sur l'utilisation de caméras de surveillance dans le centre-ville du secteur Mingan*, p. 27.

---

actuellement s'adresser au directeur de la protection incendie et de la sécurité publique ou obtenir un mandat de la cour »<sup>16</sup>.

La CAI est informée de l'installation de la première caméra par un reportage radiophonique de Radio-Canada diffusé le 3 juillet 2002. Elle annonce, le 5 juillet 2002, qu'elle procédera à une enquête pour vérifier la conformité de la vidéosurveillance de la Ville aux dix règles minimales d'utilisation des caméras de vidéosurveillance dans les lieux publics, adoptées en mai 2002. Un enquêteur est dépêché sur les lieux entre le 23 juillet et le 1<sup>er</sup> août 2002. Dans le rapport final d'enquête, déposé en octobre 2002, on signale qu'aucune affiche n'indique la présence des caméras. De plus, on reproche à la Ville de ne pas avoir mené de consultation auprès de ses partenaires du secteur social ou scolaire. La Ville reconnaît que les incendies surviennent surtout le soir, la nuit et la fin de semaine. Le rapport d'enquête signale aussi l'absence d'une étude des risques et des dangers ainsi que d'une analyse de la criminalité. La CAI ordonne à la Ville de débrancher la caméra et de ne pas en installer d'autres tant qu'elle n'aura pas démontré leur nécessité.<sup>17</sup>

Dans une lettre adressée à la CAI, des responsables de la Ville de Baie-Comeau commentent les résultats et les conclusions de l'enquête. Ils soutiennent que les intervenants du milieu et les gens d'affaires rencontrés lors de l'enquête « ne peuvent émettre leur opinion de façon adéquate » sur les mesures suffisantes à mettre en place pour résoudre les problèmes de délinquance et de criminalité « car ils ne sont pas au fait de tous les moyens qui ont été mis en application afin d'améliorer la situation »<sup>18</sup>. Parmi les mesures mises de l'avant pour remédier au problème rencontré lors de la période estivale 2001, on y mentionne, entre autres, la présence de patrouilles à pied et de patrouilles statiques, des opérations impliquant des véhicules banalisés « minounes » pour surveiller le secteur ainsi qu'une collaboration au programme des travailleurs de rues. Le directeur de la sécurité publique et de la Division incendie de la Ville « a tenté de mettre sur pied un comité d'approches stratégiques en résolution de problèmes en invitant la population par la voie des journaux à une rencontre.

Aucune personne ne s'y est présentée »<sup>19</sup>. À la suite de l'intervention de la CAI, la Ville installe quatre affiches informant la population de la présence de caméras.

---

<sup>16</sup> *Ibid.*, p. 15.

<sup>17</sup> Au moment de l'enquête, une seule caméra est en opération. Une deuxième sera installée par la suite, avant le dépôt du dernier rapport de l'enquêteur.

<sup>18</sup> Ville de Baie-Comeau, lettre envoyée le 30 septembre 2002 à la Commission d'accès à l'information, p. 2.

<sup>19</sup> *Idem.*

---

Dans une lettre envoyée le 10 décembre 2002 au maire de Baie-Comeau, la CAI conclut que la première caméra de vidéosurveillance installée dans le secteur Mingan respecte dans l'ensemble les règles minimales d'utilisation des caméras de vidéosurveillance édictées en mai 2002. Toutefois, elle demande à la Ville « de revoir d'ici six mois, en concertation avec les intervenants du milieu, l'opportunité de maintenir la caméra de surveillance ou de limiter son usage à une période de l'année, telle la saison estivale, et qu'elle fasse rapport à la Commission; de surseoir à l'installation de toute nouvelle caméra de surveillance jusqu'à la production du rapport mentionné au paragraphe précédent »<sup>20</sup>.

En réponse aux exigences de la CAI, le conseil municipal de Baie-Comeau décide de former un comité de concertation avec des intervenants de différents secteurs (municipal, social, économique, sécurité publique et santé) et demande à la CAI de reporter jusqu'au 15 septembre 2003 la date du dépôt du rapport afin de donner le temps au comité de réaliser la concertation avec les intervenants du milieu. Le comité de concertation convoque la population de Baie-Comeau à une séance de consultation publique, le 2 septembre 2003, sur l'utilisation des caméras au centre-ville. Moins de 10 personnes s'y présentent et une seule dénonce l'installation des caméras. Des membres du comité de concertation réalisent aussi des consultations auprès de responsables d'organismes œuvrant auprès de jeunes alors qu'un questionnaire est envoyé aux commerçants pour évaluer l'impact des caméras. Le comité de concertation demande à la Sûreté du Québec et à la direction des incendies de la Ville de lui fournir des « données et statistiques sur les infractions criminelles et les incendies commis dans le secteur visé et ailleurs dans la municipalité »<sup>21</sup>.

Le comité de concertation dépose le 19 octobre 2003 son rapport à la Ville de Baie-Comeau que celle-ci transmet aussitôt à la CAI. On y souligne que la criminalité a cessé dans le secteur vidéosurveillé, notamment les incendies dans les conteneurs à ordures. On ne peut cependant démontrer hors de tout doute que cette baisse est liée à la présence des caméras. On y mentionne aussi que les enfants retournent dans les parcs et que les personnes âgées reviennent au centre ville pour prendre leur marche. On y apprend également que quatre affiches ont été apposées afin d'informer la population de la présence des caméras et que d'autres mesures ont été maintenues ou mises en place pour prévenir la délinquance et la criminalité, dont des patrouilles menées par une équipe de jeunes ou le programme des travailleurs de rue. Le comité recommande :

- le maintien des deux caméras de vidéosurveillance au centre-ville;
- le rejet pour l'instant de l'installation d'une troisième caméra dans ce secteur;

---

<sup>20</sup> Commission d'accès à l'information, lettre envoyée le 10 décembre 2002 au Maire de Baie-Comeau, p. 3.

<sup>21</sup> Ville de Baie-Comeau (2003), *Rapport du Comité de concertation ...*, p. 3.

- 
- l'adoption d'un devis d'opération des caméras de vidéosurveillance;
  - la révision annuelle de l'utilisation des caméras;
  - la diminution du nombre d'heures d'enregistrement à 16 heures entre le 15 avril et le 15 septembre et à 12 heures le reste de l'année;
  - l'amélioration des liens de communication entre les intervenants sociaux, la Sûreté du Québec et la Ville de Baie-Comeau.

Tout en soulignant la qualité du rapport que lui a soumis le comité de concertation, la CAI conclut dans une lettre envoyée le 20 novembre 2003 au greffier et responsable de l'accès à la Ville de Baie-Comeau que l'utilisation des caméras respecte les règles minimales édictées en 2002. Toutefois, le rapport comporte certains problèmes méthodologiques, signale la CAI.

Elle recommande à la Ville de poursuivre sur une base continue sa réflexion sur les mesures de remplacement à la vidéosurveillance ainsi que sur la concertation avec le milieu, notamment « en effectuant des sondages à l'occasion, non seulement auprès des commerçants, mais également auprès des différents groupes de la population qui utilisent et/ou fréquentent les secteurs touchés par la surveillance par caméras ainsi qu'auprès des organismes concernés et en s'assurant, le cas échéant, qu'une information pertinente soit transmise »<sup>22</sup>. La lettre du 20 novembre 2003 constitue la dernière intervention de la CAI dans le dossier de Baie-Comeau. Aucun autre suivi n'a depuis été fait auprès des autorités municipales de Baie-Comeau.

#### 4.1.3. CENTRE-VILLE DE MONTRÉAL

Après que le Service de police de la Ville de Montréal [SPVM] ait tenté en vain d'endiguer le trafic de drogue au centre-ville, particulièrement autour de la station de métro Berri-UQAM, l'arrondissement de Ville-Marie adopte le 6 avril 2004 une résolution qui autorise le SPVM à installer des caméras de vidéosurveillance entre le 1300 et le 1700 de la rue Saint-Denis, du 1<sup>er</sup> mai 2004 au 31 août 2004.

Par ce projet, nommé Robot-Cam, le SPVM espère dissuader les transactions de stupéfiants dans le secteur et diminuer la perpétration de divers crimes. Deux caméras sont installées le 1<sup>er</sup> mai puis deux autres à la mi-juillet. Les quatre caméras sont en opération 24 heures par jour. Les images captées sont enregistrées, puis détruites au bout de sept jours. Personne ne surveille en direct les images captées.

---

<sup>22</sup> Commission d'accès à l'information, lettre envoyée le 20 novembre 2003 au Greffier et responsable de l'accès de la Ville de Baie-Comeau, p. 3.

---

Les images enregistrées au cours de l'été 2004 ont fait l'objet d'un visionnement à cinq reprises pour retracer les auteurs de vols ou de voies de fait. Cependant, aucune de ces images n'a été utilisée dans le cadre de poursuites judiciaires. Dès son annonce publique, le projet Robot-Cam fait les manchettes. Informée par la voie des médias et à la demande de la Confédération des syndicats nationaux (CSN), la CAI décide de faire enquête afin de vérifier si le projet-pilote respecte les dix règles minimales édictées en juin 2002.

À la suite d'une investigation sur le terrain et d'une analyse des documents fournis par le SPVM, le rapport préliminaire d'enquête de la CAI signale, entre autres, les lacunes suivantes :

- imprécisions méthodologiques et analytiques dans les documents fournis<sup>23</sup>;
- absence de données sur des zones avoisinantes afin d'évaluer s'il y a eu déplacement de la criminalité;
- autres moyens moins intrusifs non envisagés ou non documentés;
- nécessité de recueillir des images 24 heures par jour non justifiée;
- absence d'affiche indiquant les coordonnées d'un responsable à joindre;
- affiches signalant la présence de caméras placées à de mauvais endroits ou mal dirigées;
- non respect du délai de conservation des images en raison de problèmes techniques;
- absence d'un système permettant de masquer certaines images lorsqu'il y a une demande d'accès;
- Absence de consultation auprès des organismes communautaires.

Le SPVM transmet à la CAI, le 13 décembre 2004, son propre rapport d'évaluation. Produit à l'interne, ce rapport s'appuie sur des entrevues et des consultations menées auprès de policiers, de commerçants et de résidents ainsi que sur des données statistiques sur la criminalité et sur l'utilisation du système. La majorité des commerçants rencontrés estiment qu'il y a eu des changements positifs depuis l'installation des caméras sur la rue St-Denis. Ils souhaitent non seulement que le projet se poursuive à l'été suivant, mais qu'il couvre un territoire plus étendu. Ils souhaitent aussi qu'il y ait surveillance des écrans afin d'avertir plus rapidement la police lors d'un incident. Les huit résidents rencontrés proposent que les caméras ne se limitent plus au seul effet dissuasif appelé à s'estomper avec le temps, mais qu'elles deviennent également un outil répression du crime.

---

<sup>23</sup> Par exemple, « [p]lusieurs types de délits sont pris en compte de façon agrégée dans les statistiques, de sorte qu'il est difficile d'évaluer l'impact éventuel des caméras sur les différents types de délits » (CAI, 2005, p. 29).

---

Ils recommandent aussi que les caméras filment à l'année et que d'autres soient déployées dans les rues résidentielles avoisinantes. Certains résidents vont jusqu'à proposer que des caméras soient installées sur le mur de leur maison. Enfin, constatant un déplacement des activités reliées à la vente de stupéfiants vers d'autres secteurs avoisinants, les résidents « se disent très préoccupés par les jeunes des HLM de la rue Saint-André qui, selon eux, font l'objet d'activités de recrutement »<sup>24</sup>.

À la lumière des interventions policières, le SPVM soutient que le nombre d'arrestations reliées à la possession de stupéfiants a baissé depuis le début du projet, passant de 72 durant les mois de mai et juin à 27 durant les mois de juillet et août 2004. Selon les policiers interrogés, l'effet dissuasif des caméras « s'est rapidement estompé et les activités des revendeurs ont repris.

Toutefois, ils ont observé un changement dans le comportement des revendeurs »<sup>25</sup>. Ceux-ci marchent avec les clients et se déplacent hors du périmètre de visionnement des caméras. Quant aux crimes perpétrés dans la zone vidéosurveillée entre 2003 et 2004, ils sont en baisse de 33 % pour les crimes contre la personne et de 30 % pour les crimes contre la propriété.

Les précisions additionnelles apportées par le SPVM ne permettent pas de combler les lacunes méthodologiques et empiriques signalées dans le premier rapport et de justifier la nécessité de recourir à la vidéosurveillance. De plus, selon la CAI, le SPVM n'apporte aucune précision sur l'absence de concertation avec les autres intervenants du milieu et sur la possibilité de recourir à des approches concertées avec ces autres intervenants. Elle réitère l'importance de recourir à une évaluation réalisée de façon indépendante qui associerait les principaux acteurs du quartier. Selon la CAI, aucun élément nouveau ne permet d'appuyer la nécessité de recueillir et de conserver des images par caméra.

Qui plus est, la CAI souligne que le SPVM devra dorénavant respecter les nouvelles « Règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics », publiées le 7 juin 2004.

Le 12 mai 2005, la CAI est informée par la Ville de Montréal que le projet Robot-Cam sera remis en opération durant l'été 2005. La CAI mandate deux enquêteurs pour vérifier si la deuxième phase du projet Robot-Cam respecte les nouvelles règles de la vidéosurveillance publiées en 2004. Les enquêteurs de la CAI rencontrent des membres du SPVM qui leur remettent divers documents d'évaluation et d'analyse produits par le service de police. Ces documents précisent que le projet Robot-Cam ne se limite plus

---

<sup>24</sup> Police de Montréal (2004), *Projet Robot-Cam. Rapport d'évaluation*, préparée par la Section Recherche et planification stratégique, p. 14.

<sup>25</sup> *Ibid.*, p. 18.

---

seulement à dissuader le crime. L'assignation d'agents au visionnement en direct des caméras permet de viser aussi la répression du crime au moment où ceux-ci surviennent. Ces « agents techniques de surveillance » visionnent les images captées du jeudi au dimanche de 18h à 2h 30.

Durant l'été 2005, quatre caméras de vidéosurveillance filment encore une partie de la rue St-Denis. La période couverte est élargie, commençant le 28 juin pour se terminer le 31 octobre. Les images sont enregistrées pour une période de sept jours lorsqu'il n'y a pas de visionnement en direct.

Dans un rapport préliminaire d'enquête, déposé le 12 avril 2006, la CAI souligne que certaines lacunes constatées en 2004 ont été corrigées. De nouvelles affiches ont été apposées, avisant les passants qu'ils entrent dans une zone vidéosurveillée et indiquant un numéro de téléphone et une adresse pour contacter le SPVM. Les périodes d'enregistrement ont été réduites au profit de périodes de visionnement en direct. Le SPVM a ajouté à son système de caméras un mécanisme de brouillage qui permet de masquer certaines images qui relèvent du domaine de la vie privée. Différentes mesures de remplacement ou complémentaires à la vidéosurveillance semblent avoir été envisagées.

Le rapport de la CAI souligne aussi que le SPVM a créé un comité de vigie et d'éthique en vidéosurveillance qui « est chargé de veiller (vigie) au-delà du respect des obligations législatives et réglementaires à ce que le système de vidéosurveillance mis en place par le SPVM ne porte pas atteinte aux libertés fondamentales »<sup>26</sup>. Les mesures d'accès aux enregistrements ont été resserrées et les mécanismes de destruction des enregistrements ont été respectés. Enfin, le SPVM a mandaté des chercheurs externes pour évaluer le projet Robot-Cam. Selon ces chercheurs, les caméras ont contribué à diminuer de 10% le nombre de vols et d'agressions et de 15 % le nombre d'arrestations pour vente de drogues illicites. Quant aux points de vente avoisinants non assujettis à la vidéosurveillance, ils seraient devenus plus actifs que ceux qui opèrent sous le regard de la caméra, de l'avis des chercheurs. Ils estiment qu'il n'existe pas de motifs sérieux pour restreindre l'action des caméras à la seule saison estivale. De plus, ils soulignent qu'il serait plus efficace d'enregistrer en continu plutôt que de demander aux opérateurs de caméras de démarrer l'enregistrement quand des motifs raisonnables permettent de croire qu'une infraction est sur le point d'être commise. Quant aux mesures visant à restreindre l'accès aux enregistrements, elles seraient si contraignantes, soutiennent les chercheurs, qu'elles auraient nuit à la coordination effective des opérateurs de caméras et des patrouilleurs.

---

<sup>26</sup> Commission d'accès à l'information (2006), *Rapport préliminaire d'enquête concernant l'installation de caméras de surveillance par le service de police de la ville de Montréal*, p. 17.

---

Par ailleurs, les chercheurs suggèrent la mise en place d'un nombre beaucoup plus important de caméras de vidéosurveillance dans les lieux jugés criminogènes du centre-ville.

Cependant, la CAI questionne de nouveau certains choix méthodologiques privilégiés par les chercheurs, tout en signalant des imprécisions dans le devis d'évaluation, dans la démarche d'analyse et dans les conclusions de l'étude. On remet également en cause certains résultats de l'évaluation, notamment la baisse de 15 % de vente de drogues illicites et de 10 % de vols et d'agressions. Avant d'ajouter d'autres caméras, souligne la CAI, il faut d'abord démontrer la nécessité des quatre caméras déjà en place, ce qui n'a pas encore été fait.

Au surplus, les documents fournis par le SPVM, incluant le rapport d'évaluation des chercheurs externes, ne permet ni d'évaluer l'impact réel de la vidéosurveillance sur la vie privée, ni de statuer sur un possible débordement de la criminalité vers les zones avoisinantes, souligne la CAI. Le SPVM n'est pas non plus en mesure de démontrer que l'enregistrement est la solution appropriée pour l'ensemble des plages non couvertes par le visionnement en direct, précise-t-elle. Si d'autres solutions de remplacement ou complémentaires à la vidéosurveillance ont été envisagées, les informations fournies aux enquêteurs ne permettent pas de procéder à des vérifications quant à leur efficacité. Enfin, le SPVM donne peu d'indication sur les efforts déployés pour obtenir la participation des organismes communautaires concernés par la vidéosurveillance, indique-t-on dans le rapport d'enquête. En somme, si un certain nombre de règles ont été respectées, d'autres ne le sont pas.

L'arrondissement Ville-Marie et le SPVM décident de poursuivre le projet Robot-Cam à l'été 2006. Selon le chargé de communications de l'arrondissement Ville-Marie, « [i]l y aura de nouvelles caméras et la durée d'observation augmentera, car les deux phases du projet-pilote ont donné des résultats plus que satisfaisants ».<sup>27</sup> De fait, le nombre de caméras passe de quatre à six. À la demande des policiers du poste de quartier 38, l'arrondissement du Plateau-Mont-Royal décide, lors d'une résolution prise le 5 juin 2006, d'installer à son tour des caméras de vidéosurveillance. On prévoit alors installer dix-huit caméras le long du boulevard Saint-Laurent, entre les rues Sherbrooke et Duluth afin de réduire le nombre de crimes violents, notamment à la sortie de bars, et atténuer les problèmes liés aux gangs de rue. On espère aussi diminuer la revente de drogue et les méfaits contre la propriété (ex : graffitis). Comme dans le cas de la rue St-Denis, les caméras fonctionneront durant l'été. Le projet de caméras sur le boulevard Saint-Laurent est finalement retardé d'un an en raison de travaux de réfection sur cette rue.

---

<sup>27</sup> Éric Clément, « La vidéosurveillance prend de l'ampleur La police installe des caméras sur Saint-Laurent et en augmente le nombre rue Saint-Denis », *La Presse*, 6 juin 2006.

---

À l'été 2007, le SPVM installe les dix-huit caméras du boulevard St-Laurent et deux sur la rue St-Hubert. Selon le responsable des projets de caméras de vidéosurveillance au SPVM :

Des analyses sont en cours pour en installer un peu partout dans l'île ... Tous les secteurs sont à l'étude, on veut sortir du centre-ville ... Nous consultons les 39 commandants de quartier à ce propos ... Pour l'instant, la vidéosurveillance est toujours au stade de projet ... Mais l'an prochain, on veut qu'elle s'intègre à nos pratiques régulières.<sup>28</sup>

Pour justifier ce déploiement de vidéosurveillance, le SPVM rappelle que les crimes contre la propriété ont chuté de 38 % et les crimes contre la personne de 8% grâce aux caméras installées sur St-Denis. La CAI n'a entrepris aucune démarche depuis l'annonce des nouvelles installations de vidéosurveillance à Montréal.

## **4.2. Quelques constats sur les trois projets**

### 4.2.1. UN CONTEXTE ÉCONOMIQUE ET SOCIAL FAVORABLE À LA VIDÉOSURVEILLANCE

Les trois projets de vidéosurveillance décrits ci-haut ont été fortement soutenus par les commerçants et, dans le cas du projet Robot-Cam de Montréal, par des groupes de résidents habitant dans le secteur. Au-delà de la prévention ou de la répression par les services policiers de certains crimes et délits, la vidéosurveillance vise à favoriser le développement d'activités commerciales au centre-ville tout en assurant une certaine qualité de vie et la quiétude dans le quartier. Des citoyens du centre-ville de Montréal souhaitent d'ailleurs que l'on installe des caméras non seulement sur la rue St-Denis, mais aussi dans les rues résidentielles avoisinantes.

Subissant les pressions des commerçants et de certains résidents du centre-ville, les autorités publiques peuvent être tentées de ne pas limiter la vidéosurveillance aux actes criminels pour viser toute forme d'incivilité. Dans un contexte de revitalisation urbaine, les risques de glissement de finalité sont présents, dont celui de voir la vidéosurveillance se muter en un mécanisme de nettoyage urbain et de répression auprès des groupes marginaux qui dérangent, comme les prostitués, les toxicomanes, les itinérants et les jeunes de la rue. Par ailleurs, le déploiement des caméras de surveillance dans les trois projets à l'étude ne s'est pas fait sans susciter certaines craintes et oppositions. Par exemple, la CSN s'est fortement objectée, dès le départ, au projet Robot-Cam de Montréal, tandis que la Ligue des droits et libertés a demandé l'intervention de la CAI

---

<sup>28</sup> Émilie Côté, « Des caméras de surveillance sur le boulevard Saint-Laurent », *La Presse*, 2 mai 2007.

---

deux ans après l'installation des premières caméras à Sherbrooke. Différents citoyens ont aussi exprimé leurs inquiétudes par la voie des journaux. Malgré une couverture médiatique souvent négative, les projets n'ont pas suscité de mobilisation citoyenne suffisamment efficace pour contrer l'installation des caméras.

La seule véritable mobilisation, organisée par Pierre-Hughes Boisvenu à l'été 2005, visait au contraire une utilisation plus intensive de la vidéosurveillance en suggérant l'enregistrement des images au centre-ville de Sherbrooke. De façon générale, la population semble plutôt silencieuse face à l'installation et l'intensification de la vidéosurveillance dans les lieux publics. Cette indifférence présumée se traduit, entre autres, par de faibles taux de participation aux consultations publiques sur la question.<sup>29</sup> Malgré son silence, la population tend à percevoir la vidéosurveillance comme un outil utile de répression contre le crime, même si son efficacité est loin d'être démontrée.<sup>30</sup>

#### 4.2.2. UNE PROLIFÉRATION DE PROJETS DE VIDÉOSURVEILLANCE DANS LES LIEUX PUBLICS

De façon générale, la vidéosurveillance est souvent proposée comme première mesure de sécurité à la suite de crimes, où figurent entre autres les attentats terroristes qui retiennent l'attention soutenue des médias et qui fait craindre le pire à la population. La croyance populaire veut que si la vidéosurveillance ne prévient pas nécessairement le crime, elle peut à tout le moins permettre d'identifier les criminels et conduire à leur arrestation. Comme le signalent Norris et Armstrong<sup>31</sup>, l'opinion publique est influencée par le rôle très médiatisé des caméras dans la détection des crimes; les médias et les caméras seraient faits l'un pour l'autre.

Les crimes contre la personne, les crimes contre la propriété et les attentats perpétrés par des groupes terroristes sont les principaux motifs invoqués pour justifier l'installation de caméras de vidéosurveillance. Des événements comme ceux du 11 septembre 2001

---

<sup>29</sup> Voir, en particulier, les projets de Baie-Comeau et de Robot-Cam. Cette faible participation des citoyens à des consultations publiques a aussi été constatée dans un projet de vidéosurveillance au centre-ville de Toronto (Voir Randy Lippert, (2009), « Camera Surveillance, Privacy Regulation, and Informed Consent », dans *Report on Camera Surveillance in Canada, Part One*, produit par Surveillance Camera Awareness Network (SCAN), p. 31.

<sup>30</sup> La majorité des études disponibles semblent en effet indiquer que la vidéosurveillance n'a qu'un faible impact sur la criminalité ou la délinquance dans les espaces publics ouverts, comme les rues, particulièrement en ce qui concerne les crimes contre la personne ou les infractions non préméditées. De plus, la vidéosurveillance est peu efficace si elle n'est pas organisée pour permettre la répression des infractions. Comme tend à le montrer le projet Robot-Cam, l'effet préventif tend à s'estomper sans répression. Cependant, la vidéosurveillance semble plus efficace dans les espaces fermés, comme les stationnements et les centres commerciaux.

<sup>31</sup> Norris, Clive and Gary Armstrong (1999). *The Maximum Surveillance Society: The Rise of CCTV*, Oxford, Berg publishers.

---

à New York ou les attentats du métro de Londres en juillet 2005 pressent les autorités publiques et politiques à agir et à resserrer la surveillance dans les lieux publics de manière à sécuriser la population.

Les transports publics sont particulièrement visés par ce type de pression populaire. Par exemple, profitant d'un important financement du gouvernement fédéral, des villes canadiennes comme Toronto, Calgary et Montréal<sup>32</sup>, comptent prochainement déployer de nombreuses caméras — ou l'on déjà fait — dans leur système de transports en commun. Outre les transports en commun, comme le métro, les autobus et les trains de banlieue, on retrouve aussi de plus en plus de caméras de vidéosurveillance dans les autobus scolaires<sup>33</sup> et les taxis<sup>34</sup>.

#### 4.2.3. DES ANALYSES PRÉALABLES À L'INSTALLATION DE LA VIDÉOSURVEILLANCE INSATISFAISANTES

À la lumière des conclusions d'enquêtes menées par la CAI, différentes activités d'analyse préalables à l'installation des caméras de vidéosurveillance semblent avoir été négligées par les responsables des trois projets de vidéosurveillance.

Plus précisément, les analyses justifiant l'installation des caméras de surveillance se sont avérées parfois imprécises, notamment quand il s'agit de documenter les éléments suivants : la nécessité de recourir à vidéosurveillance pour résoudre un problème circonscrit (règle 1); la nature et la gravité des problèmes à régler (règle 2 et 3); les mesures de remplacement envisagées pour enrayer le problème avant de recourir à la vidéosurveillance (règle 4) et les effets de la vidéosurveillance sur la vie privée et sur le déplacement de la criminalité afin de s'assurer que les bénéfices en matière de sécurité sont supérieurs aux inconvénients (règle 5). À la décharge des organismes publics, on peut comprendre qu'il n'est pas facile de démontrer *a priori* les effets réels de la vidéosurveillance sur les crimes visés ainsi que ses effets non désirés, dont le déplacement de la criminalité vers des zones voisines. La CAI veut faire respecter les

---

<sup>32</sup> Grâce à une enveloppe de 4 millions de dollars du gouvernement fédéral dans le cadre d'un programme de mesure anti-terrorisme, la Société de transport de Montréal (STM) compte installer 500 caméras supplémentaires pour augmenter la surveillance dans les couloirs du métro, pour un total de 1700 caméras. La STM entend aussi équiper de caméras des autobus qu'elle recevra en 2009. Depuis 2005, environ 50 autobus sont déjà équipés de caméras dans le cadre d'un projet pilote visant à améliorer la sécurité des passagers et des chauffeurs.

<sup>33</sup> L'utilisation de vidéosurveillance dans les autobus scolaires prend de l'ampleur au Québec depuis quelques années. Plusieurs commissions scolaires au Québec ont déjà recours à ce moyen pour rétablir la discipline dans les véhicules.

<sup>34</sup> Des villes canadiennes, comme Ottawa et Windsor, ont autorisé les entreprises de taxis à équiper leurs véhicules de caméras de surveillance.

---

principes de la nécessité et de la proportionnalité lorsqu'elle demande aux organismes publics d'être plus précis au sujet de la nature et de la gravité des problèmes à résoudre et de documenter et expliquer pourquoi ces problèmes ne peuvent être résolus par d'autres mesures moins intrusives. La vidéosurveillance ne doit pas être perçue comme la panacée à tous les problèmes de criminalité dans les lieux publics.

La faiblesse des analyses préalables entraîne un certain laxisme dans l'utilisation des caméras, en particulier quand il s'agit 1) de limiter l'usage des caméras à des périodes, à des lieux, à des événements ou à des circonstances où se produisent habituellement les crimes (règle 11), 2) de limiter l'enregistrement des images lorsque c'est nécessaire (règle 12) et, 3) de minimiser les effets de la vidéosurveillance sur la vie privée en évitant, par exemple, de diriger les caméras vers des endroits privés (règle 13).

La CAI a d'ailleurs été obligée à quelques reprises d'amener les organismes à restreindre leur utilisation de la vidéosurveillance, incluant l'enregistrement des images, dans le temps et dans l'espace. Une situation criminogène réelle pour laquelle la vidéosurveillance pourrait s'avérer efficace n'exige pas nécessairement de tout filmer et tout enregistrer en tout temps.

#### 4.2.4. DES INTERVENTIONS QUI DÉPASSENT L'EXPERTISE DE LA CAI

La nécessité et la proportionnalité se mesurent en bonne partie par l'évaluation de l'efficacité non seulement de la vidéosurveillance, mais aussi des mesures de remplacement et des mesures complémentaires à la vidéosurveillance. Des mesures autres que la vidéosurveillance peuvent parfois s'avérer efficaces dans certains contextes criminogènes et s'avérer moins intrusives sur le plan de l'atteinte à la vie privée. Il est alors normal que la CAI se demande si l'utilisation de mesures de remplacement (règle 4) ou si l'utilisation de mesures complémentaires en cours de vidéosurveillance (règle 8) ont été envisagées par les organismes publics avant d'installer les caméras.

Par contre, on peut se demander dans quelle mesure la CAI possède l'expertise requise pour suggérer la nature des mesures de remplacement ou complémentaires qui devraient être adoptées ou pour juger, en dernière analyse, de leur efficacité en matière de sécurité publique. Les corps de police ne sont-ils pas mieux placés pour suggérer de telles mesures et pour juger de leur efficacité? Une fois que les caméras installées sont en opération, les organismes publics sont tenus de réviser périodiquement la nécessité de recourir à la vidéosurveillance (règle 20).

Cette procédure d'évaluation périodique repose sur le principe selon lequel la vidéosurveillance constitue un projet en constante révision et non une infrastructure permanente. Or, dans quelle mesure la CAI doit-elle apprécier la rigueur méthodologique des devis et la validité des résultats des évaluations, comme elle l'a fait

---

pour le projet Robot-Cam? A-t-elle l'expertise pour procéder à de telles appréciations? À supposer qu'elle détient cette expertise, une telle analyse n'excède-t-elle pas sa compétence et ses pouvoirs? Les appréciations méthodologiques de deux évaluations périodiques du projet Robot-Cam ont plutôt démontré que cette tâche pouvait être très exigeante pour la CAI.

#### 4.2.5. UNE EFFICACITÉ DIFFICILE À MESURER DE FAÇON PRÉCISE

Comme l'a montré le projet Robot-Cam, une évaluation périodique de la vidéosurveillance peut être un exercice complexe au plan méthodologique. En effet, une telle évaluation implique que l'on distingue les effets directs de la vidéosurveillance des effets générés par d'autres mesures, y compris les mesures complémentaires.

Autre élément de complexité méthodologique, l'évaluation doit tenir compte des effets de déplacement de la criminalité vers les zones voisines.

Il ne faut pas se surprendre que peu d'études ont pu mesurer de façon précise le degré d'efficacité de la vidéosurveillance dans des projets particuliers.<sup>35</sup> Cela soulève la question du fardeau de la preuve empirique exigée dans le cadre de l'évaluation de l'efficacité de la vidéosurveillance. Jusqu'où les organismes doivent-ils faire la démonstration scientifique, voire statistique, de la nécessité et, par conséquent, de l'efficacité du système de vidéosurveillance mis en place? À quelle fréquence doivent-ils réaliser ces évaluations périodiques? Est-ce à chaque année, comme le suggère la CAI et les autres commissaires provinciaux, ou aux cinq ans, comme l'exige la CNIL? Dans quelle mesure des évaluations d'orientation plus qualitative peuvent aussi convenir pour évaluer l'efficacité de la vidéosurveillance et pour justifier la nécessité de poursuivre ou de cesser son utilisation? Par exemple, peut-on envisager une approche de type recherche-action qui impliquerait les différentes parties prenantes dans le processus d'évaluation? Le fait de recourir à un évaluateur externe à l'organisme responsable est-il suffisant pour garantir l'objectivité nécessaire? Peut-on généraliser les conclusions d'une évaluation d'un projet particulier à d'autres projets, comme on semble le faire avec le projet Robot-Cam?<sup>36</sup>

---

<sup>35</sup> À cet égard, la Commissaire de l'Ontario soutient que "without an ability to control the many factors that influence outcomes and the context and mechanisms that produce these outcomes, it is not surprising that the results of earlier evaluations have been mixed, conflicting and, at times, contradictory" (Cavoukian, A. (2008) *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report*, Information and Privacy Commissioner of Ontario. Disponible à l'adresse suivante: <http://www.ipc.on.ca/images/Findings/mc07-68-ttc.pdf>.

<sup>36</sup> À notre avis, une telle pratique apparaît contestable puisque que les effets de la vidéosurveillance varient non seulement dans le temps, mais aussi selon le contexte d'utilisation et les types de crimes qui ont cours.

---

#### 4.2.6. UNE IMPLICATION ÉLARGIE POUVANT ENRICHIR LA RÉFLEXION

Selon la règle 7, « [l]a finalité de la vidéosurveillance doit être transparente ». Pour ce faire, « [l]es populations concernées doivent être consultées et impliquées avant la prise de décision ». Il apparaît important que la consultation et le processus de décision qui en découle n'impliquent pas seulement les groupes habituellement en faveur de l'installation des caméras, comme les associations de commerçants et les associations de résidents du centre-ville. La présence de groupes communautaires et d'associations qui défendent divers intérêts, dont ceux des groupes marginaux, peut aussi contribuer à l'enrichissement du débat. Est-il opportun que les diverses parties prenantes consultées participent à l'ensemble des étapes du projet, de sa conception à son évaluation? Chose certaine, la confrontation d'une multiplicité de points de vue demeure un des meilleurs remparts face à des dérives susceptibles de porter atteinte à la liberté d'individus. Jusqu'où doit-on aller dans la diversité des parties prenantes afin de favoriser un débat élargi? Plus les groupes impliqués tiendront des points de vue variés, voire divergents, plus ils seront vigilants face à d'éventuels dérapages ou atteintes à la vie privée.

Or, il arrive que les groupes communautaires ou de défense d'intérêts des marginaux refusent de participer à la démarche de consultation et de prise de décision, comme ce fut le cas pour le projet Robot-Cam de Montréal.

N'appartient-il pas à l'organisme responsable de la vidéosurveillance de mettre en place des conditions de participation favorables, notamment en permettant un dialogue ouvert et une recherche de compromis? Quant à la consultation du public, l'expérience montre jusqu'ici que cette pratique ne remporte pas beaucoup de succès. Peut-être faudrait-il prévoir d'autres formes de consultation plus souples et plus accessibles que des convocations à des consultations publiques traditionnelles qui nécessitent de se déplacer à des moments précis. Les consultations en ligne pourraient-elles être une avenue supplémentaire à considérer pour susciter le débat auprès des populations concernées ou de leurs représentants?

#### 4.2.7. UNE POLITIQUE ÉCRITE MIEUX ENCADRÉE

Incitées à le faire par la CAI, les trois municipalités en cause ont adopté une politique interne écrite sur l'utilisation de la vidéosurveillance. La politique sert à préciser les règles que les organismes publics s'engagent à suivre lors de l'utilisation de la vidéosurveillance, à définir les objectifs poursuivis et les mesures mises en place (ex : mesures de sécurité et audits) pour assurer la conformité à la loi et aux règles.

Les organismes publics devraient-ils être mieux guidés quant au contenu de ces politiques? On sait que certains commissaires provinciaux donnent plus précisions en indiquant, par exemple, un délai maximum de conservation des enregistrements et une fréquence acceptable pour réaliser des évaluations périodiques et des *audits*. La même

---

question se pose quant aux critères visant à sécuriser l'accès aux visionnements et aux enregistrements. La politique sur l'utilisation de la vidéosurveillance peut constituer un élément de responsabilisation auprès des différents intervenants dans la mesure où elle fait l'objet d'un engagement des responsables et intervenants du système qui doivent la respecter.

La sensibilisation et la formation des opérateurs à l'égard de cette politique devient un élément clef pour assurer une utilisation appropriée de la vidéosurveillance tant sur le plan éthique (ex : éviter d'exercer une surveillance discriminatoire ou déplacée) que fonctionnel (ex : faciliter une communication efficace entre les opérateurs et les policiers). Ceux qui observent les écrans ne doivent pas devenir de simples téléspectateurs. Les policiers ont également intérêt à recevoir une formation adaptée pour favoriser une utilisation éthique et efficace de la vidéosurveillance.

#### 4.2.8. UN SUIVI IRRÉGULIER ET UN ENCADREMENT INSUFFISANT DES PROJETS DE VIDÉOSURVEILLANCE

Le plus souvent, la CAI apprend l'existence des nouveaux projets de vidéosurveillance lorsqu'ils font la manchette des journaux et des nouvelles télévisées ou qu'une plainte est logée auprès de ses instances. Cet état de fait est d'autant plus inquiétant que le nombre de projets de vidéosurveillance ne cesse d'augmenter dans les lieux publics, sans que la CAI n'en soit saisie autrement que dans un contexte d'urgence.

Comment la CAI pourrait-elle intervenir de façon cohérente, efficace, si déjà elle éprouve des difficultés à assurer le suivi des trois seuls projets de vidéosurveillance sur lesquels elle a enquêté? La CAI ne dispose pas vraiment de mécanismes efficaces pour s'assurer que les organismes publics responsables de ces projets respectent les obligations que la loi leur impose.

Pour exercer un suivi plus étroit des projets de vidéosurveillance, la CNIL exige que les organismes lui déclarent toute installation de vidéosurveillance dans les lieux publics. Si la CAI s'engageait dans cette voie, la déclaration pourrait-elle, par exemple, être accompagnée de la politique d'utilisation de la vidéosurveillance par l'organisme ainsi que des principaux éléments de justification qui garantissent les principes de nécessité et de proportionnalité. La CAI devrait-elle en plus accorder son autorisation préalable à l'installation de la vidéosurveillance? La charge de travail déjà excessive que porte la CAI ne le permet pas pour l'instant. Doit-on pour autant éliminer l'étape de l'autorisation préalable? Dans le cas français, cette responsabilité est dévolue au préfet depuis

---

1995<sup>37</sup>, pendant que la CNIL se réserve l'autorisation au préalable des systèmes de vidéosurveillance qui font intervenir la biométrie et autres mécanismes d'identification numérique.

En vertu de la règle 17, la CAI interdit dans le cadre de la vidéosurveillance le recours aux technologies d'identification numériques et au couplage de données qui peut en résulter. Devant la prolifération des caméras biométriques, en particulier dans les aéroports, doit-on interdire à jamais ces formes d'identification intelligente? La *Loi concernant le cadre juridique des technologies de l'information*<sup>38</sup> semble autoriser indirectement ce type d'outil en prévoyant une compétence d'encadrement de la CAI au sujet des banques de données biométriques. Les caméras intelligentes qui détectent et analysent les mouvements, comme on en retrouve dans les métros et les aéroports, doivent-elles, elles aussi, être soumises aux mêmes interdictions? Voilà toute une série de questions auxquelles nous allons tenter de répondre dans les sections suivantes.

La figure 1 qui suit reprend les principaux constats dégagés de l'analyse comparée des guides canadiens et de l'expérience québécoise en matière de vidéosurveillance.

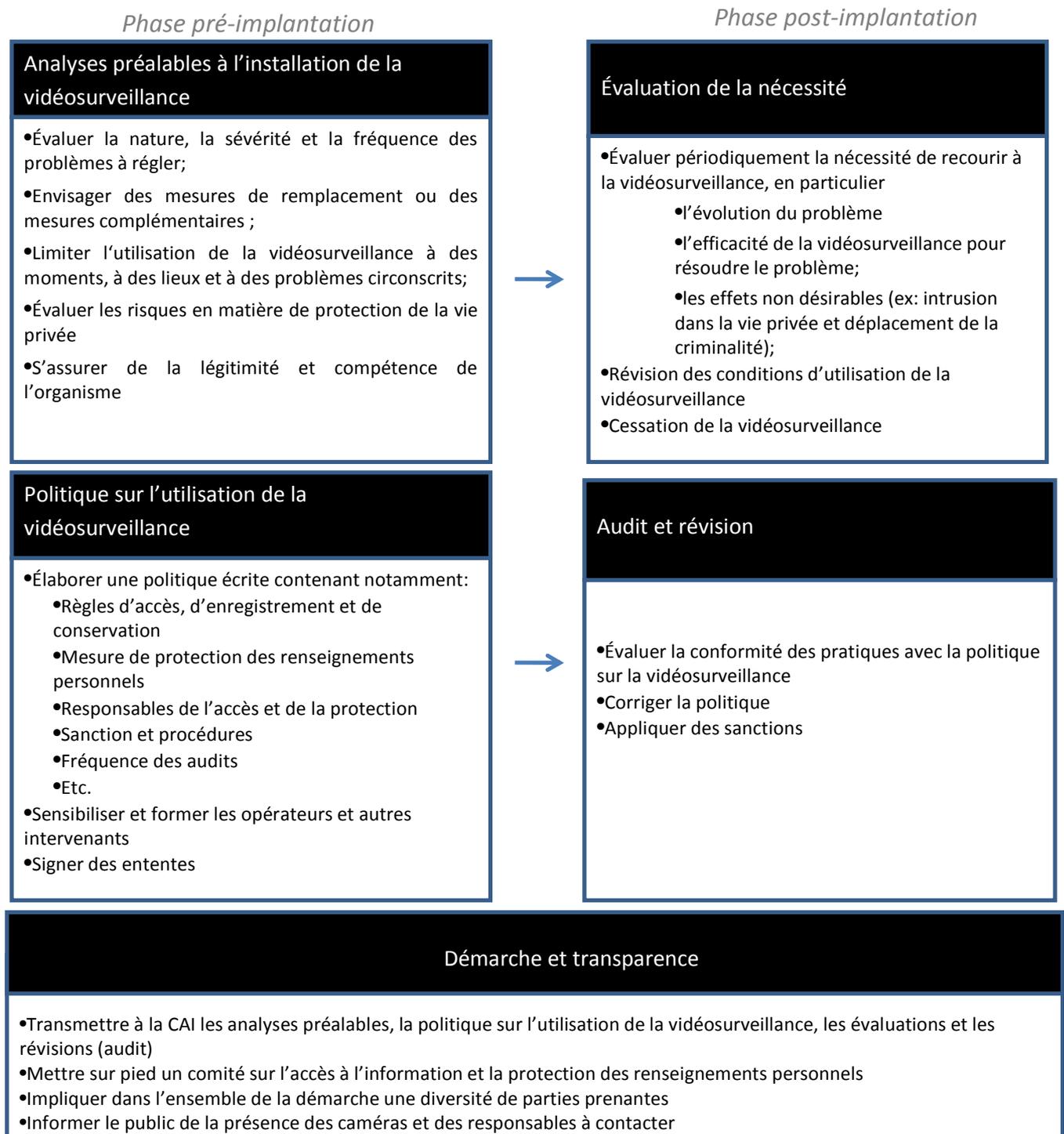
---

<sup>37</sup> Une commission départementale de vidéosurveillance étudie tous les nouveaux dossiers d'installation et rend un avis au Préfet pour autorisation. Les autorisations sont délivrées pour une durée de cinq ans. Selon la Ligue des droits de l'homme, les membres des commissions départementales se déplaceraient très rarement sur le terrain pour procéder aux vérifications nécessaires. De plus, la non-permanence de ces commissions, leur petite taille et leur composition en font des instances mal outillées pour développer une expertise technique requise et pour vérifier la nécessité de chacun des systèmes. On reproche aussi au préfet d'être en position de juge et partie, autorisant des systèmes de vidéosurveillance après avoir participé à leur élaboration et à leur financement. Un groupe de travail sur la vidéosurveillance a présenté au Sénat français, en 2008, un rapport dont la principale recommandation vise à réunir sous une seule autorité, la CNIL, les compétences d'autorisation préalable en matière de vidéosurveillance. Les auteurs suggèrent de réaffecter à la CNIL les montants correspondants au coût des commissions départementales.

<sup>38</sup> L.R.Q., c. C-1.1.

Figure 1

## Cadre de gestion de la vidéosurveillance pour les organismes publics



---

## 5. Compétence, pouvoirs, structure et fonctions

### 5.1. Entre compétence, pouvoirs et fonctions

Il est utile de distinguer la compétence d'un organisme public de ses pouvoirs et fonctions, même si ce n'est pas toujours facile et que la loi, la doctrine ou la jurisprudence les assimilent trop souvent.

La compétence désigne le domaine d'intervention attribué à un organisme public. La législation utilise souvent des termes différents pour désigner la compétence d'un organisme public. Les exemples les plus courants sont la «juridiction» [anglicisme pour un usage qui s'écarte de la fonction judiciaire ou quasi-judiciaire<sup>39</sup>], l'« attribution »<sup>40</sup>, la « mission »<sup>41</sup> ou la « fonction »<sup>42</sup>.

Le terme précis de compétence est d'utilisation plutôt récente en droit québécois. Pour prendre un exemple significatif de l'utilisation du terme de *compétence* dans la législation, la *Loi sur les compétences municipales*<sup>43</sup> confie aux municipalités des responsabilités en matière de culture et loisirs, de distribution et traitement de l'eau, de salubrité du milieu, de collecte et traitement des ordures, de sécurité civile et incendie ou de transport, pour nommer les principales *compétences* confiées aux autorités municipales. Pour s'acquitter de ses responsabilités dans ces domaines, la municipalité dispose de certains *pouvoirs*, comme le pouvoir d'expropriation, un pouvoir réglementaire et un pouvoir de taxation. Le *pouvoir* représente donc l'outil de puissance publique dont est doté l'organisme public pour s'acquitter de ses *compétences*.

La distinction entre *pouvoirs* et *fonctions* est encore plus difficile à faire, ces deux termes étant le plus souvent assimilés. La doctrine reconnaît normalement les quatre grandes fonctions de l'État comme étant les fonctions législative, exécutive, administrative et judiciaire. Cette caractérisation des fonctions publiques omet la fonction de surveillance et de contrôle, puisque selon la doctrine classique, cette fonction est assimilée à la fonction judiciaire. Pensons par exemple au pouvoir de surveillance et de contrôle de la Cour supérieure<sup>44</sup>. Le développement considérable du droit administratif au cours du XXe siècle et la diversité des fonctions quasi-judiciaires sont ainsi mis en veilleuse.

---

<sup>39</sup> Usage correct dans «fonction juridictionnelle», comme dans a. 53, 2<sup>o</sup>, LAI.

<sup>40</sup> Comme à l'article 64 LAI.

<sup>41</sup> Comme à l'article 9 de la *Loi sur l'administration publique*, L.R.Q., c. A-6.01, ou l'article 4 de la *Loi sur l'Agence des partenariats public-privé du Québec*, L.R.Q., c. A-7.002.

<sup>42</sup> Comme à l'article 28 LAI.

<sup>43</sup> L.R.Q., c. C-47.1.

<sup>44</sup> Articles 33 et 846 et suivants du *Code de procédure civile*, L.R.Q., c. C-25.

---

Tentons ici de faire les distinctions utiles entre compétences, fonctions et pouvoirs de la CAI. La CAI cumule deux grands domaines de compétence : 1) l'accès à l'information auprès des organismes publics et 2) la protection des renseignements personnels que ces organismes détiennent. En comparaison, on sait que l'instance fédérale a scindé ces deux compétences pour les confier à deux instances distinctes, soit le Commissariat à l'accès à l'information du Canada et le Commissariat à la protection de la vie privée du Canada, tout comme la France, qui a créé deux commissions séparées : la CADA [Commission d'accès aux documents administratifs], responsable de l'accès à l'information, et la CNIL [Commission nationale de l'informatique et des libertés], chargée de la protection de la vie privée.

La CAI assume par ailleurs deux *fonctions* dont chacune opère dans ces deux domaines de compétences : une fonction juridictionnelle et une fonction de surveillance et de contrôle, comme nous le précisons à la section 5.2. Enfin, la CAI dispose de certains *pouvoirs* (section 6) pour remplir ses fonctions dans les deux domaines de compétence.

## **5.2. La structure de la CAI et sa double fonction**

La CAI met en œuvre deux fonctions pour s'acquitter de ces deux domaines de compétence : la fonction de surveillance et de contrôle et la fonction juridictionnelle. Ces deux fonctions relèvent du champ quasi-judiciaire. La CAI est responsable, depuis ses origines, de cette double fonction. Elle doit s'acquitter d'une fonction juridictionnelle par laquelle elle entend, à l'exclusion de tout autre tribunal, les demandes de révision faites en vertu de la LAI (a. 134.2 LAI). La Commission assume également une mission de contrôle et de surveillance (a. 122 à 134 LAI), sans oublier la mission de promotion<sup>45</sup> en matière d'accès à l'information et de protection des renseignements personnels.

Cette dimension bi-fonctionnelle de la Commission a régulièrement suscité des questions au cours de son histoire. Les critiques ont été particulièrement importantes lors de la Commission parlementaire de l'automne 2003 qui faisait suite au dépôt du Rapport quinquennal de la Commission en 2002<sup>46</sup>. On se souviendra particulièrement du rapport présenté par Me Raymond Doray, à la demande du Ministère des Relations

---

<sup>45</sup> Qui pourrait s'apparenter davantage à une mission d'éducation auprès des organismes publics quant à leurs responsabilités et de sensibilisation auprès des citoyens quant à leurs droits.

<sup>46</sup> Commission d'accès à l'information, *Une réforme de l'accès à l'information : le choix de la transparence*, 184 p. plus les annexes.

---

avec les citoyens et de l'immigration<sup>47</sup>, souligné au rapport final de la Commission de la Culture chargée de la consultation<sup>48</sup>.

La Commission de la Culture n'a pas retenu les propositions de réformes structurelles à la CAI qui lui auraient valu de perdre sa fonction juridictionnelle au profit du Tribunal des droits de la personne du Québec. Le Législateur a, par contre, entendu certains de ces commentaires au moment de l'adoption, en 2006, d'amendements importants à la LAI, afin de réduire le risque de crainte raisonnable de partialité de la CAI découlant du cumul de ses fonctions.

À la suite de la présentation du projet de loi 86 en décembre 2004, la *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*<sup>49</sup> était sanctionnée le 14 juin 2006. Les modifications adoptées consacrent notamment que la fonction juridictionnelle et la fonction de surveillance doivent relever de deux sections distinctes de la Commission.

Ainsi, la loi prévoit depuis juin 2006, à son article 103, que la CAI comporte deux sections : une section de surveillance et une section juridictionnelle. Afin d'en assurer une certaine étanchéité, l'article 104 édicte que la résolution de l'Assemblée nationale qui nomme les membres de la CAI doit identifier à laquelle des deux sections appartiennent les membres, à l'exception du président et du vice-président.

Ces considérations sont importantes, puisqu'elles visent à instaurer des mécanismes permettant à la CAI de ne pas mettre en péril ses garanties d'impartialité de sa fonction juridictionnelle dans l'exercice de sa fonction de surveillance. Rappelons que les critiques soulevaient notamment qu'une décision prise dans le cadre de la fonction de surveillance et de conseil pouvait placer la Commission dans une situation d'apparence de partialité lorsqu'elle était par la suite appelée à se prononcer dans sa fonction d'adjudication de demandes en révision. En matière de vidéosurveillance, un tel risque d'apparence de partialité pourrait survenir dans l'hypothèse où un système de vidéosurveillance faisait l'objet d'une procédure s'apparentant à une approbation préalable de la Commission à la lumière de critères qu'elle adopte elle-même, pour faire l'objet, par la suite, d'une plainte pour non-conformité à la loi.

---

<sup>47</sup> Raymond Doray, *La mise en œuvre des lois d'accès à l'information gouvernementale et de protection des renseignements personnels au Québec : analyse critique et perspectives de réforme organisationnelle*, juin 2003, 54 p.

<sup>48</sup> Commission de la culture, *Observations, conclusions e recommandations à la suite de la consultation générale et des auditions publiques à l'égard du document intitulé : Une réforme de l'accès à l'information : le choix de la transparence*, Rapport final, mai 2004, 54 p. plus les annexes, p. 44-45.

<sup>49</sup> L.Q. 2006, c. 22.

---

La surveillance de l'application par les organismes publics des *Règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, développées et adoptées par la CAI, relève de sa section de surveillance, dénommée «Direction de l'analyse et de l'évaluation» [ci-après DAE] à son organigramme publié dans son site web<sup>50</sup>. Nous allons donc dans ce rapport limiter nos commentaires et concentrer notre analyse aux *pouvoirs* qu'exerce cette Direction, dans le souci de préserver l'étanchéité prévue par la loi avec la section juridictionnelle et l'objectif de maintenir l'impartialité tout comme l'apparence d'impartialité de la Commission.

### **5.3. La répartition de la compétence en matière de protection des renseignements personnels entre les organismes publics et la CAI**

#### 5.3.1. LES ORGANISMES PUBLICS ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les organismes publics sont régis par la LAI et doivent respecter les normes qui y sont édictées en matière de protection des renseignements personnels, et notamment dans le cadre de l'implantation de systèmes de vidéosurveillance. Dès qu'un système de vidéosurveillance envisagé par l'organisme public est susceptible de générer la production de renseignements personnels<sup>51</sup>, il est soumis à la compétence de la CAI qui assure le contrôle du respect du caractère confidentiel des renseignements produits. Si les renseignements sont versés dans un document ou un fichier, d'autres responsabilités de l'organisme public sont alors activées, comme les règles de la finalité, de la nécessité et de la transparence, interpellant alors la compétence de la CAI pour en assurer le respect.

La production d'un renseignement personnel dans un document ou un fichier exige normalement un enregistrement, une conservation ou un traitement des images filmées. C'est la raison pour laquelle l'enregistrement de la vidéosurveillance revêt une grande importance, puisque cette décision accroît la compétence de la Commission face au système de vidéosurveillance mis en place par l'organisme public.

---

<sup>50</sup> Il faut souligner que l'organigramme publié sur le site web de la CAI (consulté le 13 mars 2009) ne permet pas d'identifier clairement la section juridictionnelle ni de déterminer à laquelle de la section de la surveillance ou de la section juridictionnelle sont rattachés les membres, contrairement à ce que prévoit la LAI.

<sup>51</sup> L'identification de la personne doit être possible pour répondre à la définition du renseignement personnel, qu'il y ait enregistrement ou non. Ainsi, les caméras qui nous permettent de voir de haut les rues achalandées de certaines grandes agglomérations, comme Montréal (Montrealcam.com) ou la surveillance des grands axes routiers par Transports Québec, ne génèrent pas nécessairement de renseignements personnels au sens des règles de protection des renseignements personnels.

---

Les organismes publics sont donc soumis à des responsabilités en vertu de la LAI afin d'assurer la protection des renseignements personnels. Ces responsabilités peuvent se résumer ainsi :

#### *Confidentialité*

- Les renseignements personnels sont confidentiels, sauf exceptions (a. 53 LAI);
- La communication d'un renseignement personnel est prohibée sans le consentement de la personne concernée, sauf exceptions (a. 59 LAI, qui réfère aux exceptions qui exigent certaines précautions, comme ententes et inscriptions à un registre);
- Un organisme ne doit pas communiquer hors Québec un renseignement qui ne bénéficiera pas d'une protection équivalente à celle prévue par la LAI (a. 70.1 LAI);
- Un corps de police peut communiquer un renseignement à un autre corps de police (a. 61 LAI);
- Un renseignement personnel n'est accessible, au sein de l'organisme, qu'aux personnes qui ont qualité pour le recevoir dans le cadre de leurs fonctions (a. 62 LAI);
- L'organisme public doit protéger les renseignements personnels en mettant en œuvre les mesures édictées par règlement du gouvernement (a. 63.2 LAI) [Nous inscrivons ce principe sous les quatre rubriques de responsabilités qui incombent aux organismes publics, puisque la disposition habilitante s'exprime de façon générale et peut toucher toutes les mesures de protection des renseignements personnels].

#### *Sécurité*

- Des mesures de sécurité propres à assurer la protection des renseignements personnels doivent être mises en place (a. 63.1 LAI);
- L'organisme public doit protéger les renseignements personnels en mettant en œuvre les mesures édictées par règlement du gouvernement (a. 63.2 LAI).

#### *Nécessité et proportionnalité*

- L'organisme public ne peut recueillir qu'un renseignement personnel qui est nécessaire à l'exercice de ses attributions ou à la mise en œuvre d'un programme dont il a la gestion (a. 64 al.1 LAI);

- 
- Un organisme public doit prévoir une directive pour la communication sans le consentement de la personne concernée d'un renseignement personnel pour prévenir un acte de violence, dont un suicide ou s'il existe un motif raisonnable de croire à un danger imminent de mort ou de blessures graves (a. 59.1, al. 3, a. 60 LAI). La directive adoptée doit préciser que l'organisme devra vérifier le caractère nécessaire du renseignement et le caractère urgent et dangereux de la situation. À défaut, l'organisme doit refuser la communication du renseignement. La communication doit être inscrite à un registre (a. 60 al.4 et 60.1 al. 2);
  - L'organisme public doit protéger les renseignements personnels en mettant en œuvre les mesures édictées par règlement du gouvernement (a. 63.2 LAI).

#### *Transparence et finalité*

- Toute personne a droit d'être informée de l'existence dans un fichier d'un renseignement personnel la concernant et a droit d'en recevoir communication (a. 83 LAI);
- La collecte d'information auprès d'un sujet se fait en précisant, oralement ou par écrit, pour qui, pour quelles fins et à qui seront transmis les renseignements, selon la méthode de cueillette. Cet article ne s'applique pas à un organisme chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois (a. 65 LAI);
- Un renseignement ne doit être utilisé que pour les seules fins pour lesquelles il a été recueilli (l'exception exige une inscription au registre) à moins que cet autre usage ne soit compatible ou au bénéfice clair de la personne concernée, ou encore pour un usage nécessaire à l'application d'une loi au Québec (a. 65.1 LAI);
- Un renseignement personnel doit être détruit lorsque la fin pour laquelle il a été recueilli est accomplie (a. 73 LAI);
- Un organisme public doit maintenir à jour un inventaire de ses fichiers de renseignements personnels (a. 76 LAI);
- L'organisme public doit protéger les renseignements personnels en mettant en œuvre les mesures édictées par règlement du gouvernement (a. 63.2 LAI).
- La loi assigne donc aux organismes publics qui souhaitent mettre en place un système de vidéosurveillance la responsabilité première de s'acquitter de ces obligations et responsabilités en matière de protection des renseignements personnels concernant les sujets filmés par les caméras de vidéosurveillance.
- On constate également que chacune de ces catégories de responsabilités ou règles en matière de protection des renseignements personnels se présente sous la forme de normes générales édictées dans la loi, tout en permettant au gouvernement d'en préciser la nature par pouvoir réglementaire.

---

### 5.3.2. LE RÔLE DE SURVEILLANCE ET DE CONTRÔLE DE LA CAI

Par rapport aux renseignements recueillis par les systèmes de vidéosurveillance des organismes publics, le rôle de la CAI en est un de surveillance et de contrôle afin d'assurer le respect des obligations auxquelles sont soumis les organismes publics, énoncées à la section précédente. L'article 122.1 alinéa 1 LAI énonce que «La Commission a pour fonction de surveiller l'application de la présente loi (...), pendant que l'alinéa 2 précise qu'elle est «aussi chargée d'assurer le respect (...) de la protection des renseignements personnels.»

La DAE de la CAI est responsable de la mise en œuvre de cette fonction de contrôle et de surveillance. Si les organismes publics doivent respecter les prescriptions de la loi et de ses règlements, la Commission doit en assurer le respect, dans la mesure des pouvoirs que lui confère la loi pour s'acquitter de ce devoir. Nous allons à la prochaine section analyser plus en détails les pouvoirs dont dispose la CAI pour s'acquitter de sa fonction de surveillance et de contrôle des mesures de protection des renseignements personnels que doivent prendre les organismes publics en vertu de la loi et de ses règlements.

---

## 6. Les pouvoirs de la CAI pour exercer son rôle de surveillance

La LAI prévoit deux catégories de pouvoirs permettant à la CAI d'exercer sa compétence en matière de surveillance et de contrôle de la protection des renseignements personnels par les organismes publics : des pouvoirs spécifiques pour répondre à des situations particulières et des pouvoirs généraux. Nous allons d'abord nous pencher sur les pouvoirs spécifiques afin d'analyser si ces pouvoirs peuvent être mis en œuvre par la CAI afin de surveiller la mise en place de systèmes de vidéosurveillance dans les lieux publics par les organismes publics soumis à la LAI. Nous verrons que les pouvoirs spécifiques de la CAI visent surtout des communications entre organismes sans le consentement de la personne concernée.

### 6.1. Les pouvoirs spécifiques de la Commission

Le principe de base de la protection des renseignements personnels repose sur le caractère confidentiel des renseignements personnels qui ne peuvent être communiqués que sous le consentement de la personne concernée. La LAI prévoit des situations qui font exception à cette règle de l'exigence du consentement de la personne concernée. C'est à l'intérieur de ce type de situations que, dans certains cas, la CAI dispose d'un pouvoir particulier d'intervention ou de contrôle de la communication.

#### 6.1.1. APPROBATION PRÉALABLE OU AVIS FAVORABLE DE LA COMMISSION AU SUJET D'UNE ENTENTE DE COMMUNICATION ENTRE ORGANISMES

L'approbation ou l'avis préalable de la CAI est requis lorsqu'un organisme public prévoit transmettre ou partager des renseignements personnels avec un autre organisme public. Ce type de transfert doit faire l'objet d'une entente entre les organismes. Cette entente doit être transmise à la CAI pour approbation préalable ou avis favorable.

L'article 68 LAI prévoit qu'un organisme public peut communiquer un renseignement sans le consentement de la personne visée si «cette communication est nécessaire à l'exercice des attributions de l'organisme receveur», à la mise en œuvre d'un programme, dans le cadre de la prestation de services ou pour le bénéfice clair de la personne concernée. Cette communication doit se faire par entente dont le contenu est précisé à l'alinéa 2 de l'article 68 LAI.

L'article 70 LAI ajoute que cette entente doit être transmise à la CAI pour avis.

L'article 68.1 LAI prévoit le même pouvoir d'avis préalable dans le cas de couplage de fichiers, nécessaire à l'application d'une loi, mais non prévu expressément à la loi. L'entente de couplage doit se faire par entente soumise à la CAI pour avis (a. 70 LAI). La CAI rend son avis motivé dans les 60 jours. Sur avis défavorable, le gouvernement

---

peut, sur demande, approuver l'entente à la suite de la publication à la *Gazette officielle* pour commentaires dans les 30 jours. Les documents pertinents doivent ensuite être déposés à l'Assemblée nationale.

De plus, un organisme public qui décide de confier à un autre organisme public les obligations que la LAI lui impose, doit le faire par entente soumise à l'approbation de la Commission (a. 172 LAI).

La LAI prévoit donc des situations bien précises où un organisme public doit demander une autorisation préalable de la CAI avant de procéder. Ces situations sont toutes liées à la communication d'un renseignement personnel à un autre organisme public, sans le consentement de la personne concernée.

#### 6.1.2. TRANSMISSION D'UNE ENTENTE OU INFORMATION PRÉALABLE À LA COMMISSION

L'article 64 LAI prévoit un pouvoir analogue, mais légèrement différent, dans le cas où un organisme recueille un renseignement personnel nécessaire à l'exercice de ses compétences dans le cadre d'une collaboration ou d'une mission commune avec un autre organisme. L'entente doit être transmise à la CAI (a. 64 al. 2) et n'entre en vigueur que 30 jours après sa réception par la CAI, donnant l'occasion à la Commission d'intervenir si elle le juge à propos, sans que l'approbation préalable ne soit formellement exigée. La CAI est ainsi présumée avoir consenti à la communication si elle ne s'est pas manifestée dans les 30 jours de la réception du projet de communication. Il en est de même pour les ententes de couplage de fichiers formellement autorisées par la loi (a. 68.1 alinéa 3 LAI).

La Commission doit également être informée au préalable lorsqu'un organisme public veut transmettre à un autre organisme public un renseignement concernant l'identité d'une personne pour permettre la collecte d'informations déjà colligées (a. 66 LAI). Cette communication doit de plus être inscrite dans un registre (a. 67.3 LAI).

Enfin, la *Loi concernant le cadre juridique des technologies de l'information* accorde un pouvoir analogue d'information préalable à la CAI. En effet, selon l'article 45 de cette loi, toute «banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la CAI», avant même sa création. La CAI peut alors rendre toute ordonnance concernant sa confection, son utilisation, sa consultation, sa communication ou sa conservation pour assurer la protection de la vie privée.

#### 6.1.3. EXIGER LA TENUE ET L'INSCRIPTION DANS UN REGISTRE

La plupart des communications mentionnées ci-haut exigent par ailleurs une inscription à un registre tenu par l'organisme public (a. 67.3 et 64 al. 3 LAI). Un organisme public doit également inscrire au registre tout usage autre que celui pour lequel le

---

renseignement a été saisi, en autant que cet usage soit compatible avec le premier, pour l'application de la loi ou au bénéfice clair de la personne concernée (a. 65.1, 67, 67.1, 67.2, 68 et 68.1 LAI).

#### 6.1.4. OBLIGATION POUR UN ORGANISME PUBLIC D'ADOPTER DES DIRECTIVES

L'article 59.1 LAI prévoit une obligation spécifique imposée aux organismes publics d'adopter une politique interne pour la communication de renseignements personnels sans le consentement de la personne concernée, lorsque cette communication vise la prévention d'un acte de violence, dont le suicide. Une telle politique devrait alors préciser comment s'évalue le danger imminent de mort ou de blessures graves menaçant une personne ou un groupe justifiant la communication sans le consentement de la personne.

Cette situation est la seule mentionnée à la LAI qui rend obligatoire l'adoption d'une politique interne de l'organisme public pour préciser son pouvoir discrétionnaire de gestion des renseignements personnels dans le respect des dispositions de la LAI. L'obligation légale pour l'organisme public d'adopter une politique interne permet à la CAI de vérifier si l'organisme public s'est acquitté de son obligation.

Cela pose la question de la possibilité pour la Commission d'exiger des organismes publics de se munir d'une politique interne en matière de vidéosurveillance, en l'absence de l'inscription à la loi (ou dans un règlement) d'une obligation analogue à celle que l'on retrouve pour la prévention d'urgence d'actes de violence appréhendés.

#### 6.1.5. LA CAI PEUT-ELLE EXERCER SES POUVOIRS COMME SI ELLE EXIGEAIT UNE AUTORISATION PRÉALABLE À LA VIDÉOSURVEILLANCE?

Les pouvoirs spécifiques dont dispose la CAI pour assurer le respect de la LAI sont de deux catégories<sup>52</sup>. Le premier type de pouvoir concerne une approbation ou une intervention préalable de la CAI à une communication de renseignements personnels. La loi prévoit dans un cas un pouvoir explicite d'approbation préalable (a. 68, 68.1 et 70 LAI), tandis que ce pouvoir est sous-entendu dans un autre cas, soit celui où la CAI dispose d'un délai de 30 jours après que l'organisme l'eut obligatoirement avisée, pour intervenir et faire connaître ses objections (a. 64, 66 et 68.1 al. 3 LAI). Toutes les situations visées par ce pouvoir concernent une entente de communication de renseignements personnels sans le consentement de la personne.

---

<sup>52</sup> On écarte ici le pouvoir de surveiller le respect de l'inscription à un registre lorsque requis par la loi, qui ne vise pas non plus les systèmes de vidéosurveillance, à moins d'une transmission d'informations à un autre organisme public ou une utilisation autre que celle prévue lors de la mise en place du système.

---

Ces situations ne peuvent pas être assimilées à la décision d'un organisme public de mettre en place un système de vidéosurveillance pour s'acquitter de ses propres compétences, sans transmission à un autre organisme public, comme les systèmes de vidéosurveillance mis en place par les autorités municipales et policières de Baie-Comeau, de Sherbrooke et de Montréal.

On peut donc soutenir qu'une action de la Commission équivalant à une demande d'autorisation préalable à la mise en œuvre d'un système de vidéosurveillance serait *ultra vires* des pouvoirs de la CAI.

L'inscription explicite à la LAI du pouvoir d'autorisation préalable pour d'autres situations permet de supposer qu'il n'est pas disponible pour des situations étrangères à celles visées par la loi, comme pour la mise en place d'un système de vidéosurveillance. Autrement dit, si le législateur avait voulu soumettre les organismes publics à un pouvoir d'autorisation préalable de la CAI pour la mise en œuvre d'un système de vidéosurveillance, la loi ou les règlements l'auraient énoncé de façon explicite. Comme ce n'est pas le cas, il faut comprendre que la Commission ne saurait s'appuyer sur la loi pour exiger des organismes publics qu'ils se soumettent à une telle autorisation préalable.

#### 6.1.6. LA COMMISSION DISPOSE-T-ELLE D'UN POUVOIR RÉGLEMENTAIRE OU DE DIRECTIVE GÉNÉRALE EN MATIÈRE DE VIDÉOSURVEILLANCE?

La deuxième catégorie de pouvoirs spécifiques de la CAI concerne la vérification de l'adoption d'une politique ou directive interne de l'organisme public. Ce pouvoir spécifique découle de l'obligation particulière faite à l'organisme public d'adopter une directive dans un cas précis. Il revêt ici un intérêt certain puisque la CAI s'en prévaut dans le cadre de son document *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, lorsqu'elle suggère aux organismes publics de se doter d'une politique d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics. On peut noter que si la CAI suggère l'adoption d'une telle politique, elle ne l'impose pas, ce qui est sans doute sage à la lumière de la précédente analyse.

En effet, l'obligation d'adoption de directives internes n'est précisée que pour la communication de renseignements visant à prévenir un acte de violence. Lorsque la loi impose à un organisme public d'adopter en pareilles circonstances une politique interne, il va de soi que la CAI dispose alors du pouvoir de vérifier si l'organisme public s'est muni d'une telle politique interne. Comme la loi n'impose pas aux organismes publics

---

l'adoption d'une politique interne en matière de vidéosurveillance<sup>53</sup>, on peut supposer que la Commission ne peut qu'encourager les organismes publics à se doter d'une telle politique. La Commission pourrait-elle par ailleurs disposer du pouvoir de l'imposer, en dépit du silence de la LAI à ce sujet? La question est importante et nous allons tenter de proposer une réponse.

Un organisme public peut toujours adopter une politique ou une directive interne pour préciser le pouvoir discrétionnaire que lui confère la loi ou un règlement<sup>54</sup>. Par ailleurs, si la loi prescrit que ce pouvoir doit être exercé par la voie réglementaire, l'organisme doit alors user du règlement et non pas de la directive administrative, au péril de la nullité de la directive<sup>55</sup>.

Dans le cas des *Règles* adoptées par la CAI, il faut comprendre qu'on parle de directives, politiques ou d'un guide qui s'adresse non pas à l'organisme qui l'édicte, mais à d'autres organismes soumis au pouvoir de contrôle et de surveillance du premier. Quel est le statut juridique d'un tel outil administratif?

Il est important de vérifier dans un premier temps l'encadrement du pouvoir réglementaire prévu à la LAI. On note alors que le pouvoir d'adopter des règlements pour préciser les normes en matière de protection des renseignements personnels appartient en exclusivité au gouvernement et non pas à la CAI ou au ministre responsable de l'application de la loi.

En effet, seul le gouvernement dispose du pouvoir d'adopter des règlements concernant les mesures servant à préciser certaines obligations centrales prévues à la LAI. La LAI prévoit d'abord un pouvoir réglementaire du gouvernement pour les frais d'accès aux documents et renseignements personnels, aux articles 11 et 85 LAI, inscrits depuis l'adoption de la loi et en vigueur depuis le 1<sup>er</sup> juillet 1984. Ce pouvoir a été exercé par l'adoption du Règlement A-2.1, r. 1, remplacé en 1987 par le *Règlement sur les frais exigibles pour la transcription, la reproduction et la transmission de documents et de renseignements personnels* (L.R.Q., c. A-2.1, r. 1.1).

Aucun autre pouvoir réglementaire concernant la précision des règles d'accès à l'information ou de protection des renseignements personnels n'était inscrit à la LAI avant sa modification en 2006 par l'adoption de la *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, L.Q. 2006, c. 22 [projet de loi 86]. En vigueur depuis

---

<sup>53</sup> Un nouveau Règlement impose une telle obligation pour certains organismes publics, sujet que nous aborderons à la section 8.

<sup>54</sup> Pierre Issalys, Denis Lemieux, *L'action gouvernementale. Précis de droit des institutions administratives*, Les Éditions Yvon Blais, 1997.

<sup>55</sup> *Mead Johnson Canada c. Robillard* [1995] R.J.Q. 1089 (C.S.)

---

le 15 juin 2007, la LAI prévoit depuis un pouvoir réglementaire du gouvernement concernant la diffusion sur internet de documents (a. 16.1 LAI), et pour les mesures que doivent adopter les organismes publics pour assurer la protection des renseignements personnels (a. 63.2 LAI). Le gouvernement s'est appuyé sur ces deux dispositions habilitantes pour adopter en 2008 le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1, r. 0.2<sup>56</sup>. Dans l'exercice de ce pouvoir réglementaire, le gouvernement doit d'abord solliciter l'avis de la Commission avant l'adoption du règlement (a. 123 LAI).<sup>57</sup>

Le pouvoir réglementaire de la Commission se limite quant à lui aux règles de régie interne et de déontologie (a. 110.1 LAI). Ce pouvoir a été exercé par l'adoption du *Règlement de régie interne de la Commission d'accès à l'information* (L.R.Q., c. A-2.1, r. 1.3) et du *Code de déontologie des membres de la Commission d'accès à l'information* (L.R.Q., c. A-2.1, r. 0.1) ainsi qu'en matière de procédure et preuve devant la section juridictionnelle de la CAI (a. 137.3 LAI), pouvoir soumis à l'approbation du gouvernement et exercé par l'adoption des *Règles de preuve et de procédure de la Commission d'accès à l'information* (L.R.Q., c. A-2.1, r. 2).

On sait qu'un pouvoir réglementaire ne saurait se présumer et doit toujours être énoncé de façon explicite puisqu'il relève de la délégation du pouvoir législatif. Le pouvoir de précision des mesures de protection des renseignements personnels que doivent adopter les organismes publics étant accordé au gouvernement, on peut penser que la CAI, par le biais de sa section de surveillance et de contrôle, ne dispose pas du pouvoir de faire la même chose par voie de directive ou de guide obligatoire qui lui permettrait, au surplus, d'agir de façon à requérir l'équivalent d'une autorisation préalable.

Du moins, pourrait-on préciser, la Commission ne dispose plus de ce pouvoir de directive, depuis l'adoption en 2006 de la disposition habilitante de l'article 63.2 LAI qui confère dorénavant clairement au seul gouvernement le pouvoir de préciser par règlement les mesures de protection des renseignements personnels que doivent prendre les organismes publics soumis à la loi.

L'adoption en mai 2002 des dix règles minimales, révisées en 2004 en vingt règles, servait à pallier à l'absence, à cette époque, du pouvoir réglementaire de la loi. Nous

---

<sup>56</sup> *Gazette officielle du Québec*, Partie 2, 14 mai 2008, 140<sup>e</sup> année, no.20, p. 2081 – 2084, Décret 408-2008 du 23 avril 2008.

<sup>57</sup> L'article 28 LAI prévoit également le pouvoir réglementaire du gouvernement concernant les renseignements liés à la prévention du crime (r.1.2 : *Règlement sur les organismes publics tenus de refuser de confirmer l'existence et de donner communication de certains renseignements*). Existe aussi un pouvoir réglementaire du gouvernement qui concerne la fonction juridictionnelle de la CAI, r. 1.2.1.

---

avons discuté des difficultés d'application soulevées par cette situation au moment de l'analyse des trois projets sur lesquels la CAI a fait enquête en s'appuyant sur ses propres règles.

Nous venons donc de voir que la LAI n'offre à la Commission aucun pouvoir spécifique d'autorisation préalable, qui lui permettrait d'exiger des organismes publics qu'ils lui soumettent leur proposition de système de vidéosurveillance pour approbation avant leur mise en place. La même conclusion se dégage pour douter du pouvoir réglementaire ou de directive de la Commission pour imposer des règles de protection des renseignements personnels colligés par un système de vidéosurveillance, et ce, surtout depuis l'entrée en vigueur de l'article 63.2 LAI le 15 juin 2007. On peut également douter de la validité d'un pouvoir de la Commission d'exiger des organismes publics qu'ils se dotent d'une politique interne afin de préciser les mesures de protection avant de mettre en place un tel système, dans le but de démontrer qu'ils s'assujettissent à une procédure et à des vérifications permettant d'assurer la conformité aux obligations générales auxquelles sont soumis les organismes publics en matière de protection des renseignements personnels et aux vingt règles de la CAI.

## **6.2. Les pouvoirs généraux de la CAI**

Il faut maintenant identifier quels sont les pouvoirs généraux dont dispose la Commission pour lui permettre d'asseoir son pouvoir de surveillance et de contrôle quant au respect des règles de protection des renseignements personnels auxquelles sont soumis les organismes publics.

Les pouvoirs généraux de la Commission peuvent s'exercer de deux façons. Ils peuvent d'abord être utilisés pour vérifier si l'organisme public rencontre les exigences que la loi ou les règlements lui imposent concernant les mesures de protection des renseignements personnels. Les pouvoirs généraux peuvent aussi être exercés lorsque la Commission a des motifs de croire que les droits conférés aux personnes concernant leurs renseignements personnels ne sont pas respectés par l'organisme public. C'est dans ce contexte que la dénonciation publique ou la plainte devant la Commission joue souvent un rôle de déclencheur des pouvoirs généraux de la Commission.

### **6.2.1. POUVOIR D'ENQUÊTE ET D'INSPECTION**

La CAI dispose d'un pouvoir général d'enquête et d'inspection quant au respect de la LAI (a. 123 alinéa 1, 1<sup>o</sup> LAI) par lequel elle peut notamment autoriser un membre de son personnel ou une autre personne à agir comme inspecteur (a. 123.1 LAI).

L'inspecteur peut pénétrer à toute heure raisonnable dans les locaux de l'organisme public sous enquête, y obtenir tout renseignement ou document requis et en obtenir

---

copie (a. 123.2 LAI). L'inspecteur bénéficie de l'immunité quant aux gestes posés de bonne foi dans l'exercice de ses fonctions (a. 123.3 LAI). La Commission et son inspecteur jouissent alors des pouvoirs et immunités des commissaires nommés en vertu de la *Loi sur les commissions d'enquête*<sup>58</sup>, à l'exception du pouvoir d'ordonner l'emprisonnement (a. 129 LAI).

La Commission peut également exiger de tout organisme qu'il lui fournisse toute information qu'elle requiert sur l'application de la loi (a. 130 LAI), sans que ne soit nécessairement déclenchée une enquête formelle.

#### 6.2.2. POUVOIR D'ORDONNANCE

Au terme de son enquête, la CAI dispose d'un pouvoir d'ordonnance par lequel elle peut ordonner à l'organisme public de prendre les mesures appropriées pour se conformer aux dispositions de la loi (a. 129 LAI).

#### 6.2.3. POUVOIR DE SAISIR LE GOUVERNEMENT

Si la CAI estime que l'organisme public ne donne pas suite à ses recommandations ou à son ordonnance, elle peut en aviser le gouvernement, soumettre un rapport spécial à l'Assemblée nationale ou encore exposer la situation dans son rapport annuel (a. 133 LAI).

#### 6.2.4. PRESCRIRE DES CONDITIONS APPLICABLES À UN FICHER DE RENSEIGNEMENTS PERSONNELS

L'article 124 LAI offre à la CAI un pouvoir général de prescription de conditions applicables à un fichier de renseignements personnels où elle peut prévoir le type de renseignements qui peut y être conservé, l'usage qui peut en être fait, la nature des mesures de sécurité à prendre, les catégories de personnes qui peuvent avoir accès au fichier ainsi que toute autre condition particulière à laquelle doit être soumise la gestion de ce fichier.

La Commission pourrait-elle s'appuyer sur ce type de pouvoir pour prescrire des conditions particulières en matière de vidéosurveillance?

---

<sup>58</sup> L.R.Q., c. C-37.

---

Après avoir émis l'hypothèse que ce pouvoir pourrait servir d'assise à la Commission pour mieux encadrer l'utilisation de la vidéosurveillance<sup>59</sup>, nos dernières réflexions et analyses nous permettent d'en douter.

Le pouvoir de prescription de règles de gestion d'un fichier de renseignements personnels de l'article 124 (que la Commission n'a encore jamais utilisé depuis sa création), semble s'inscrire davantage dans le cadre d'un pouvoir d'ordonnance ciblé à un fichier pour lequel la Commission aurait conclu que des mesures de correction doivent être apportées. La formulation de l'article vise bien «un fichier» et non une «catégorie de fichiers», comme le seraient les informations colligées par vidéosurveillance.

De plus, une utilisation du pouvoir prévu à l'article 124 pour édicter des mesures générales de gestion pour les fichiers créés par vidéosurveillance s'apparenterait davantage à l'exercice d'un pouvoir réglementaire dont ne jouit pas la Commission et qui appartient en exclusivité au gouvernement, comme nous l'avons vu à la section 6.1.6. Nous devons donc conclure que le pouvoir de l'article 124 LAI ne peut pas être utilisé pour mieux encadrer de façon générale l'utilisation de la vidéosurveillance dans les lieux publics.

#### 6.2.5. COMMENT PEUVENT ÊTRE UTILISÉS LES POUVOIRS GÉNÉRAUX DE LA CAI EN MATIÈRE DE VIDÉOSURVEILLANCE?

Les pouvoirs généraux de la Commission en matière d'enquête ou d'inspection sont évidemment disponibles pour permettre à la Commission de vérifier si un organisme public respecte les prescriptions de la loi et des règlements en matière de protection des renseignements personnels colligés à partir d'un système de vidéosurveillance. Elle intervient dès lors après le fait, c'est-à-dire une fois le système en place.

C'est d'ailleurs sur cette base que la Commission a dépêché un inspecteur pour enquêter lorsqu'elle a été saisie d'une plainte ou d'informations concernant la mise en place des systèmes de Baie-Comeau, de Sherbrooke et de Montréal. Au terme de son enquête où la Commission doit respecter les règles de justice naturelle et permettre à l'organisme de présenter ses observations, la Commission peut émettre une ordonnance imposant les mesures de protection qu'elle juge appropriées.

---

<sup>59</sup> Nous avons émis cette hypothèse lors de la rencontre du 9 décembre 2008 aux bureaux de la CAI à Montréal, en présence de M. St-Laurent, M. Normand et de la Commissaire Christiane Constant. L'hypothèse a été réitérée lors de la rencontre avec tout le personnel de la Direction de l'analyse et de l'évaluation à Québec le 14 janvier 2009.

---

Nous avons observé, par l'analyse de la procédure suivie par la Commission dans le cadre de l'inspection de ces trois projets, que les lacunes du processus suivi par les autorités municipales ou policières devant mener à la décision d'installer un système de vidéosurveillance étaient à la source des principaux manquements observés par la Commission, et plus particulièrement concernant l'obligation pour un organisme public de s'assurer du caractère nécessaire, efficace et proportionnel de la mise sur pied de la vidéosurveillance.

Les pouvoirs généraux ne permettent donc pas de favoriser la prévention des possibles manquements à la loi. Nous avons aussi vu à la section 6.1.5 que la Commission ne dispose pas du pouvoir d'imposer une approbation préalable à l'implantation de tels systèmes. La Commission ne peut donc pas faire indirectement ce qu'elle ne peut faire directement, en transformant son pouvoir d'inspection de l'utilisation de quelques caméras en un pouvoir d'autorisation préalable à l'extension du système à d'autres caméras.

De plus, l'inspection menée dans les circonstances soulevées par les projets soutenus par les forces policières place trop facilement la Commission dans une situation où elle s'implique dans une analyse poussée de la meilleure méthode à prendre pour que l'organisme responsable de la vidéosurveillance s'acquitte de sa compétence propre en matière de prévention ou de répression du crime. De plus, la CAI ne peut pas utiliser ses pouvoirs généraux pour vérifier le respect par les organismes publics des vingt règles, dans la mesure où la validité juridique de ces règles est mise en doute (voir aussi section 7).

Ces observations nous permettent de soulever que le cadre juridique actuel n'est pas favorable au meilleur usage des compétences et pouvoirs de la Commission pour assurer une utilisation de la vidéosurveillance conforme aux prescriptions de la LAI.

---

## 7. Analyse des Règles d'utilisation de la vidéosurveillance

### 7.1. Statut juridique des règles

Le document intitulé *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, publié en juin 2004, ne s'appuie pas sur un pouvoir réglementaire de la Commission, comme nous l'avons souligné plus haut, à la section 6.1.6. Un tel document s'apparente alors normalement à un pouvoir de directive administrative, avec des appellations qui peuvent prendre diverses formes, comme un guide, une circulaire, une politique, etc. Le pouvoir d'adoption de directives par les organismes publics ne nécessite pas une autorisation expresse de la loi, puisque les organismes publics disposent de la capacité de préciser leurs pouvoirs discrétionnaires par de tels outils administratifs.

Ce document de la CAI présente par ailleurs une situation particulière, dans la mesure où son application n'est pas destinée à un usage interne, mais vise plutôt à lier les organismes publics qui sont soumis au pouvoir de contrôle et de surveillance de la Commission. Il n'y a pas là d'interdiction formelle, au contraire, puisqu'il est accepté qu'un organisme public puisse exprimer par le biais de son pouvoir de directive la façon dont il entend utiliser son pouvoir discrétionnaire face aux personnes externes. Par contre, nous avons vu à la section 6.1.6 que ces règles de la CAI se substituaient dans une certaine mesure au pouvoir réglementaire inscrit depuis 2006 à l'article 63.2 LAI, et était par conséquent susceptible d'être à cet égard *ultra vires* des pouvoirs de la CAI.

Il faut aussi ajouter un autre élément d'analyse. Il est également admis en droit que la simple directive ne saurait diminuer ou affecter un pouvoir discrétionnaire qui est conféré à un organisme public par la loi ou les règlements<sup>60</sup>.

Cette dimension nous amène donc à ne pas limiter notre analyse à la seule répartition des pouvoirs entre la Commission et le gouvernement du Québec, pour l'étendre également à la répartition des pouvoirs entre la CAI et les organismes publics qui sont soumis à son pouvoir de surveillance et de contrôle.

Les systèmes de vidéosurveillance des villes de Baie-Comeau, de Sherbrooke et de Montréal ont été mis en place pour prévenir, et dans une moindre mesure, pour réprimer les crimes et les infractions. La décision de procéder à l'installation des caméras de vidéosurveillance a été prise par les autorités municipales de Sherbrooke et de

---

<sup>60</sup> Le juge Le Dain écrivait que les «lignes directrices qui ne sont pas des règlements (...) ne peuvent limiter ou assujettir à des conditions un pouvoir discrétionnaire accordé par une loi (...)». *Maple Lodge Farms c. Gouvernement du Canada*, [1981] 1 C.F. 500, 513, confirmé par la Cour suprême, [1982] 2 R.C.S., 2.

---

Baie-Comeau, de qui relèvent le corps policier de Sherbrooke, ou avec lequel transige la municipalité, dans le cas de Baie-Comeau qui utilise les services policiers de la Sûreté du Québec. La décision de vidéosurveillance du projet Robot-Cam relève directement du SPVM, appuyée de l'autorisation du Conseil d'arrondissement.

Or, les municipalités ont des compétences spécifiques en matière de sécurité civile et incendie<sup>61</sup>. La *Loi sur la police*<sup>62</sup> régit les corps policiers municipaux et la Sûreté du Québec. La loi accorde aux corps policiers une compétence et des pouvoirs discrétionnaires très larges pour leur permettre de remplir leur mission de maintien de la paix, de l'ordre et de la sécurité publique par la prévention et la répression des infractions aux lois et aux règlements municipaux<sup>63</sup>. Aucun règlement adopté en vertu de la *Loi sur la police* ne restreint le pouvoir discrétionnaire dont disposent les autorités policières pour s'acquitter de leur compétence propre.

Les corps policiers impliqués dans les trois projets sont la Sûreté du Québec dans le cas de Baie-Comeau, et la police municipale dans les cas de Sherbrooke (services de niveau 2, selon l'a. 70 de la *Loi sur la police*) et de Montréal (services de niveau 5 selon la même disposition). Selon l'annexe G de la *Loi sur la police*, les corps policiers doivent, dès le premier niveau, offrir les services d'enquête concernant les voies de fait de toutes catégories, le vol qualifié, les incendies, et le trafic et la possession de drogues illicites au niveau local ou de rue. Le corps policier de niveau 2 doit y ajouter les services d'enquête sur les incendies en série, ainsi que les enquêtes pour le trafic et la possession de drogues visant les fournisseurs des revendeurs locaux ou de rue, tandis que le niveau de services 4 doit offrir un service de soutien à la surveillance électronique. Le niveau 6 (Sûreté du Québec) doit également donner les services d'enquête de cybersurveillance. Les corps policiers, y compris ceux impliqués dans les systèmes de vidéosurveillance de Baie-Comeau, de Sherbrooke et de Montréal, sont donc dans l'obligation de donner les services que la loi leur impose. Les outils à mettre en place pour rencontrer leurs obligations légales demeurent à leur discrétion et relèvent de leur compétence propre.

Le pouvoir discrétionnaire des policiers est tout de même encadré, autant par les règles générales du droit administratif que par les dispositions des chartes québécoise et canadienne en matière de protection des droits individuels.

Le pouvoir des corps policiers est également encadré par les autres dispositions législatives auxquelles sont soumis les corps policiers, dont les dispositions en matière de protection des renseignements personnels prévues à la LAI.

---

<sup>61</sup> *Loi sur les compétences municipales*, L.R.Q., c. C-47.1, a. 62 à 65.

<sup>62</sup> L.R.Q., c. P-13.1.

<sup>63</sup> Notamment aux articles 48, 50 et 69 de la *Loi sur la police*.

---

Même si les vingt règles de vidéosurveillance sous étude étaient validement adoptées (et nous avons vu que nous pouvons douter de leur validité, surtout depuis 2006), elles ne sauraient s'imposer aux corps policiers dans la mesure où elles relèvent du simple pouvoir de directive de la CAI et qu'elles sont susceptibles de restreindre de façon importante un pouvoir discrétionnaire qui appartient aux corps policiers, exercé conformément à la loi, y compris aux dispositions de la *Loi sur la police* et de la LAI.

## **7.2. Brève analyse sur le fond des vingt règles**

Le document intitulé *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics* publié en juin 2004 comprend vingt règles, suivies d'une suggestion à l'effet que les organismes qui souhaitent implanter un système de vidéosurveillance adopte une politique interne devant notamment définir un mécanisme de consultation du public avant de procéder à la vidéosurveillance.

Nous avons déjà traité de la valeur juridique douteuse d'une exigence de la CAI quant à l'adoption d'une telle politique interne. Nous venons au surplus de conclure aux sections 6.1.6 et 7.1, avant même de nous pencher de façon précise sur le contenu des règles, que de façon globale, ces règles sont sans doute *ultra vires* des pouvoirs de la CAI.

Nous proposons ici d'étudier sur le fond les vingt mesures avancées par les règles, afin d'en identifier les propositions qui pourraient présenter un intérêt pour une éventuelle intégration dans un règlement à être adopté par le gouvernement et identifier celles qui soulèvent des questions.

L'analyse des règles nous permet de voir, en vingt points, les normes que souhaite imposer la CAI aux organismes publics, dans le but de voir respectés les principes énoncés à la LAI, dans le contexte particulier d'un système de vidéosurveillance.

### **7.2.1. LES PRINCIPES DE LA NÉCESSITÉ, DE LA FINALITÉ ET DE LA PROPORTIONNALITÉ ET LES RÈGLES 1, 2, 3, 4, 5, 8, 10, 11, 12, 13, 18 ET 20**

La première règle<sup>64</sup> ainsi que la règle 10<sup>65</sup> reprennent en d'autres termes, tout aussi larges, la règle de la nécessité de l'article 64 alinéa 1 LAI et la règle de la finalité de

---

<sup>64</sup> «1) La vidéosurveillance doit être nécessaire à la réalisation d'une fin déterminée. Elle ne peut être utilisée de manière générale comme un dispositif de sécurité publique. Le problème à régler doit être identifié, récurrent et circonscrit.»

<sup>65</sup> «10) La vidéosurveillance doit être ajustée au besoin et adaptée à la situation. L'organisme public doit circonscrire son usage. Les périodes de surveillance et, éventuellement, d'enregistrement, l'espace visé et la manière dont se déroulera l'opération doivent être conçus de manière à minimiser les effets de la vidéosurveillance et à préserver le mieux possible la vie privée des citoyens.»

---

l'article 65.1 LAI. La règle 13<sup>66</sup> reprend également, sous une formulation adaptée à la vidéosurveillance, les règles de la nécessité et de la finalité prévues par la loi, sans restreindre outre mesure le pouvoir discrétionnaire des organismes publics tout en faisant référence au principe de proportionnalité.

Les règles 2<sup>67</sup> et 3<sup>68</sup> viennent resserrer ce que peut signifier la règle de la nécessité dans le contexte de la vidéosurveillance. Même si ces règles s'appuient sur les principes de la loi, les précisions apportées par directive ont pour effet de réduire le pouvoir d'appréciation dont disposent les pouvoirs policiers et municipaux quant aux moyens à prendre pour s'acquitter de leurs compétences propres. On peut douter de leur stricte validité juridique puisqu'un tel resserrement des pouvoirs discrétionnaires d'un organisme public ne peut se faire que par la voie législative ou réglementaire, qui n'appartient pas à la CAI.

---

<sup>66</sup> «13) La disposition des caméras et le type de technologie utilisée doivent minimiser les effets de la vidéosurveillance sur la vie privée des gens. Les caméras ne doivent pas être dirigées vers des endroits privés, tels une maison, des fenêtres d'immeubles, des salles de douche, les cabinets de toilette ou les vestiaires. À cette fin, la nouvelle technique informatique de masquage des lieux doit être retenue pour éviter une prise de vue d'endroits privés ou d'endroits qui ne sont pas concernés par la vidéosurveillance. Les angles de vue, le type de caméras, la fonction zoom ou arrêt sur images doivent être évalués en fonction des finalités recherchées et des moyens appropriés pour atteindre ces finalités. Il en est de même de l'utilisation d'un équipement muni d'une connexion avec un centre d'alerte ou d'intervention.»

<sup>67</sup> «2) L'objectif recherché par l'usage de la vidéosurveillance doit être sérieux et important. La prévention de délits mineurs ou la survenance de problèmes occasionnels ne peuvent justifier une intrusion dans la vie privée des personnes. La vidéosurveillance ne doit pas se révéler comme étant une solution de facilité. Les lieux ciblés doivent, notamment, être reconnus comme étant des espaces criminogènes.»

<sup>68</sup> «3) Un rapport concernant les risques concrets et les dangers réels que présente une situation au regard de l'ordre public et de la sécurité des personnes, des lieux ou des biens doit être réalisé. Ce rapport doit notamment faire état des points suivants : les événements précis, sérieux et concordants qui se sont produits; une identification claire du problème à régler; les exigences concrètes et réelles de sécurité publique en jeu; les lieux ciblés pour la vidéosurveillance et leurs liens avec les motifs invoqués; les objectifs importants, clair et précis qui ont été identifiés.»

---

La même question se pose quant à la force légale des règles 4<sup>69</sup>, 5<sup>70</sup>, 8<sup>71</sup>, 11<sup>72</sup> et 12<sup>73</sup> qui donnent des détails concernant le principe de proportionnalité développé par la doctrine et la jurisprudence, notamment en raison de l'atteinte potentielle de la collecte de renseignements au regard du droit à la vie privée protégé par les chartes. Ces règles qui relèvent ici de la simple directive administrative d'un organisme public affectent d'une façon importante le pouvoir discrétionnaire des autorités policières et municipales (sécurité civile) auxquelles la loi confère une compétence propre et des pouvoirs discrétionnaires qui y sont associés. L'interdiction de procéder à un enregistrement des images avant que l'agent qui observe ne constate qu'un crime est en train d'être commis est-elle réaliste et respecte-t-elle le pouvoir discrétionnaire des autorités policières de mettre en œuvre des mécanismes efficaces de prévention et de répression du crime?

---

<sup>69</sup> «4) Des solutions de rechange moins préjudiciables à la vie privée doivent avoir été envisagées ou mises à l'essai et s'être avérées inefficaces, inapplicables ou difficilement réalisables. Selon le problème à résoudre et les lieux concernés, d'autres solutions doivent avoir été expérimentées ou étudiées, notamment : la présence d'agents de sécurité; une patrouille à pied aux endroits névralgiques; l'implication de travailleurs ou travailleuses de rue; un service d'accompagnement à l'automobile sur demande; un meilleur éclairage de la zone à protéger; un renforcement des portes d'accès; l'installation de grilles protectrices et de systèmes d'alarme ou le marquage des objets reliés à un système d'alarme; une intervention du personnel de surveillance; la formation d'un comité de vigilance.»

<sup>70</sup> «5) L'impact réel de la vidéosurveillance doit être mesuré. Une analyse des risques au sujet de la protection de la vie privée a été complétée; les avantages et les inconvénients de la mesure doivent être soupesés de même que ses effets potentiellement pervers ou non désirés, comme le déplacement de la criminalité. L'efficacité de la mesure pour corriger la situation doit être probante.»

<sup>71</sup> «8) La vidéosurveillance doit être considérée avec au moins un des éléments énoncés à la règle 4 ou son équivalent.»

<sup>72</sup> «11) La vidéosurveillance doit être utilisée uniquement lors d'événements critiques et pour des périodes limitées. L'utilisation des caméras et l'enregistrement doivent être circonscrits à des heures de la journée et à des périodes de l'année précises correspondant aux moments forts où se produisent habituellement les crimes. À titre d'exemple, s'il est établi que les infractions sont perpétrées la fin de semaine, en soirée ou la nuit, ou lors de fêtes publiques ou d'événements précis, la vidéosurveillance ne doit pas s'étendre au-delà de ces périodes.»

<sup>73</sup> «12) Seuls les enregistrements nécessaires doivent être effectués. Lorsqu'une personne peut visionner de façon permanente l'image captée par une caméra, elle doit attendre d'avoir des motifs raisonnables de croire qu'une infraction va être commise pour démarrer l'enregistrement. Si personne ne peut visionner de façon continue les écrans, les bandes enregistrées doivent être détruites dès qu'elles ne sont plus nécessaires.»

---

La règle de la destruction des bandes enregistrées dès qu'on sait qu'elles ne seront plus nécessaires, inscrite à l'alinéa 3 de la règle 12 ainsi que la règle 18<sup>74</sup> sont tout à fait conformes à la règle prévue à l'article 73 LAI, sous une formulation différente.

La règle 20<sup>75</sup> prévoit d'une certaine façon une révision périodique du principe de nécessité. Dans la mesure où la règle ne restreint pas outre mesure le pouvoir discrétionnaire dont dispose l'organisme public d'évaluer la nécessité du système, la règle 20 s'appuie correctement sur l'article 64 qui implique une évaluation périodique d'un système de collecte d'information en continu.

#### 7.2.2. LES PRINCIPES DE LA LÉGITIMITÉ ET DE LA TRANSPARENCE ET LES RÈGLES 6, 7, 9, 15 ET 19

La règle 6<sup>76</sup> peut être associée à la règle de la nécessité et de la finalité de la LAI, en questionnant la légitimité de l'action d'un organisme public régi par sa loi propre. Même si la règle place la CAI à la frontière de sa compétence, son lien avec la règle de la finalité peut la rendre conforme à l'article 65.1 LAI.

---

<sup>74</sup> «18) Les supports d'enregistrement doivent être pris en compte dans le calendrier de conservation. Les supports d'enregistrement doivent être numérotés et datés par site ayant fait l'objet d'une surveillance. Mis à part les exigences judiciaires et les enquêtes policières ou administratives, les enregistrements sont effacés ou détruits dès que leur conservation n'est plus nécessaire.»

<sup>75</sup> «20) L'organisme public doit revoir périodiquement (au minimum sur une base annuelle) la nécessité de ses choix en matière de vidéosurveillance. À cet effet, les aspects suivants doivent être pris en considération : les motifs de départ existent toujours; les résultats escomptés sont atteints. Sinon, l'organisme public doit s'interroger sur les effets réels du procédé; les conditions d'utilisation sont toujours adéquates et adaptées à la situation; la pertinence du type de caméras utilisées ainsi que leur nombre; une solution de rechange plus appropriée et compatible avec le droit au respect de la vie privée n'est pas maintenant envisageable; le cas échéant, le nombre d'heures d'enregistrement par jour ainsi que des périodes d'enregistrement pendant la semaine ou l'année.»

<sup>76</sup> «6) L'organisme public doit s'assurer de la légitimité de ses objectifs de sorte que la finalité de la vidéosurveillance ne puisse être détournée ou déformée. Par exemple, la vidéosurveillance ne doit pas servir : à catégoriser ou hiérarchiser des groupes de personnes; à établir des distinctions selon l'appartenance raciale, religieuse, politique ou syndicale ou les comportements sexuels des individus; à étudier le comportement humain en vue d'exercer un contrôle sur ces personnes.»

---

La septième règle<sup>77</sup> ainsi que la règle 15<sup>78</sup> sont liées au principe de transparence inscrit à l'article 65 LAI, tout en demandant aux organismes publics d'agir conformément à leurs lois et règlements propres en s'assurant que la décision de mise en place de la vidéosurveillance est correctement prise par les autorités responsables.

Il est d'abord utile de préciser que le principe de transparence de l'article 65 LAI ne s'applique pas «à une enquête ou à un constat faits par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois». On peut alors poser la question de la validité de l'obligation énoncée par la Commission d'apposer des avis pour donner les informations exigées par l'article 65, lorsque l'objet de la vidéosurveillance est de prévenir le crime. Non seulement ce type d'instructions ne saurait être simplement donné par directive, mais au surplus, il ne peut contredire une règle claire et explicite de la loi.

On peut soutenir que le législateur avait en tête au moment de l'adoption de cette disposition la collecte d'information sur une forme ponctuelle, par opposition à une collecte en continu par vidéosurveillance, mais il est impossible ici d'interpréter l'exclusion d'application de l'article 65 LAI comme écartant la vidéosurveillance de l'exclusion. La loi ne distingue pas les collectes ponctuelles des collectes en continu et il est donc impossible de faire cette distinction dans l'interprétation de l'article 65 LAI.

Cette observation nous permet d'avancer l'hypothèse que même un règlement adopté par le gouvernement ne peut contredire l'article 65 LAI et imposer des règles de transparence comme celles prévues à cet article pour les systèmes de collecte d'images pour des fins d'enquête ou de constats mené par un organisme chargé de la prévention et de la répression du crime et des infractions. Il ne fait pas de doute que la collecte d'informations par vidéosurveillance se distingue de manière marquée de la collecte ponctuelle traditionnelle et justifie un cadre juridique plus exigeant qui n'est malheureusement pas disponible pour l'instant en ce qui concerne les systèmes de vidéosurveillance mis en place par les autorités municipales (y compris policières), sociosanitaires ou éducationnelles.

---

<sup>77</sup> «7) La finalité de la vidéosurveillance doit être transparente et explicite. Les populations concernées doivent être consultées et impliquées avant la prise de décision. L'utilisation de la vidéosurveillance doit avoir été approuvée par les autorités imputables de l'organisme public.»

<sup>78</sup> «15) Le public visé par cette vidéosurveillance doit être informé par tout avis approprié. Des avis doivent annoncer de manière non équivoque que l'endroit fait l'objet de vidéosurveillance avec enregistrement. Ces avis doivent : être placés à des endroits visibles, à une distance raisonnable du lieu surveillé et être d'un format requis par le contexte spatial; mentionner l'objet de la vidéosurveillance et le nom de la personne responsable.»

---

On peut par ailleurs se demander sur quelle disposition législative ou réglementaire pourrait s'appuyer la Commission pour exiger des organismes publics, et plus particulièrement des corps policiers, qu'ils consultent les populations concernées avant la prise de décision de l'implantation d'un système de vidéosurveillance pour prévenir ou réprimer le crime ou les infractions, comme le prévoit la règle 7. Rien dans la LAI ne permet à la Commission d'imposer ce type de consultation aux organismes chargés de prévenir ou réprimer les crimes ou infractions.

Ce constat ne signifie pas que la proposition n'est pas sensée et valable en termes de politique publique. La proposition vise une utilisation de la vidéosurveillance qui soit rationnelle et respectueuse des droits des personnes. Nous avons noté à la section 3.5 que cette règle de transparence et de consultation préalable est incluse sous une forme ou une autre à tous les guides étudiés des provinces canadiennes, confirmant ainsi sa légitimité. On sait par ailleurs que la légitimité n'équivaut pas toujours à la légalité, et vice versa. Nous n'avons pas procédé à l'analyse du statut juridique de ces guides hors Québec et ne pouvons pas nous prononcer ici sur la force juridique d'une telle recommandation pour les provinces hors Québec.

Notre analyse pour le Québec nous permet néanmoins de signaler l'écart observé entre légitimité et légalité qui mériterait d'être corrigé. Nous y reviendrons plus loin.

La règle 9<sup>79</sup> peut être associée à la règle de la transparence et de la responsabilité en désignant une personne responsable du projet de vidéosurveillance, chargée des règles d'équité de gestion de l'information recueillie. Elle peut être associée à une délégation administrative pour un projet de l'obligation faite par les articles 8 et 17 LAI.

La règle 19<sup>80</sup> ne pose également aucun problème puisqu'elle ne fait que répéter le droit d'accès de toute personne à un renseignement personnel qui la concerne, tel qu'inscrit à la loi.

### 7.2.3. LES PRINCIPES DE CONFIDENTIALITÉ ET DE SÉCURITÉ ET LES RÈGLES 14, 16 ET 17

La LAI prévoit explicitement les règles de confidentialité des renseignements personnels (a. 53) et la restriction de l'accès au sein d'un organisme public aux seules personnes qui ont qualité pour en recevoir communication dans le cadre de leurs fonctions (a. 62 LAI), de même que le droit d'accès de la personne concernée (a. 83 LAI). Les

---

<sup>79</sup> «9) L'organisme public doit désigner au départ une personne responsable de la collecte, de la conservation et de la communication des données recueillies au moyen de la vidéosurveillance. Cette personne doit s'assurer, à toutes les étapes, que les présentes règles sont respectées.»

<sup>80</sup> «19) Une personne a droit d'accès aux renseignements la concernant. Cette personne a droit d'accès aux enregistrements effectués conformément à la Loi sur l'accès.»

---

règles 14<sup>81</sup>, 16<sup>82</sup>, proposent une formulation de ces principes prévus par la loi en l'adaptant aux systèmes de vidéosurveillance.

Même si la formulation des règles 14 et 16 ajoute des détails importants en matière de sécurité et de respect de la confidentialité qui vont au-delà de la loi, ils n'ont pas pour effet de toucher le pouvoir discrétionnaire propre aux autorités policières et municipales en matière de sécurité des personnes et de la propriété concernant la prévention et la répression du crime et des infractions. Rien n'interdit alors à la Commission de prévoir par directive des règles de la sorte.

La règle 17<sup>83</sup> soulève par contre des questions différentes puisqu'elle aborde la question du couplage de données et l'utilisation de données biométriques. On peut poser la question de l'interdiction péremptoire de tout appariement des images colligées par vidéosurveillance lorsque la LAI soumet le couplage de fichiers à la procédure d'entente et d'autorisation préalable de la CAI lorsque nécessaire à l'application d'une loi (voir section 6.1.1).

L'utilisation des données biométriques est abordée dans la *Loi concernant le cadre juridique des technologies de l'information*.

L'article 44 de cette loi prohibe effectivement l'utilisation obligatoire de la biométrie pour confirmer ou vérifier l'identité d'un individu. Cette disposition prohibe-t-elle tout usage de la biométrie pour tenter l'identification d'individus par le couplage de données biométriques? Ce n'est pas certain, puisqu'on pourrait avancer qu'un usage par le corps

---

<sup>81</sup> «14) Les personnes assurant le fonctionnement des appareils doivent être bien au fait des règles visant à protéger la vie privée. Les personnes doivent avoir reçu la formation appropriée et connaître les limites imposées par la loi en matière de protection de la vie privée avant d'agir à titre d'opérateur. Il en va de même pour les tierces parties, soit celles ne relevant pas directement de l'autorité de l'organisme, notamment impliquées par contrat dans la vidéosurveillance.»

<sup>82</sup> «16) Les équipements utilisés et les enregistrements doivent être protégés. Le matériel enregistré doit faire l'objet de règles précises de conservation en sorte que la confidentialité des données soient protégée. Des mesures de sécurité doivent être mises en place afin de restreindre l'accès au poste de visionnement et aux enregistrements aux personnes expressément autorisées à cet effet. Un nombre limité de personnes autorisées peuvent accéder aux locaux hébergeant les équipements et visionner les enregistrements.»

<sup>83</sup> «17) L'utilisation des enregistrements doit être limitée. Sous réserve des exceptions prévues à la LAI, les enregistrements ne doivent pas être communiqués aux tiers. À cet égard, l'interconnexion des systèmes de surveillance, que ce soit par internet ou autrement, constitue une communication à un tiers. Les enregistrements ne doivent pas faire l'objet d'associations d'images et de données biométriques, notamment à l'aide de logiciels de consultation automatique d'images ou de la reconnaissance faciale. Les enregistrements ne doivent pas être appariés, couplés ou partagés avec d'autres fichiers, ni servir à constituer des banques de données.»

---

policier de l'information tirée d'images filmées par vidéosurveillance, couplées à des données de biométrie, ne servirait pas à confirmer ou vérifier l'identité d'une personne au sens de la *Loi concernant le cadre juridique des technologies de l'information*, mais plutôt à émettre une hypothèse d'identité dans le cadre d'un pouvoir d'enquête et qui devra être confirmée par les autres étapes de l'enquête et d'autres méthodes.

La disposition de l'article 44 doit s'interpréter dans le contexte de cette loi qui vise la sécurité juridique des communications au moyen de documents, sans égard à son support (a. 1). La loi instaure des mécanismes pour assurer l'intégrité des documents et établir un lien sûr entre un document et une personne lorsque cette personne doit confirmer son identité. L'article 44 fait suite à l'article 42 qui inscrit les articles suivants dans le contexte où «la loi exige de fournir une attestation, une carte, un certificat, une pièce ou une preuve d'identité ou autre document servant à établir l'identité d'une personne». C'est dans ce contexte, peut-on arguer, qu'il est interdit d'exiger de la personne qu'elle ne se soumette à un processus d'identification qui fait appel à une mesure biométrique. On ne peut que lui en offrir le choix, à la condition que la mesure fasse appel au minimum de caractéristiques et que la personne puisse avoir pleine conscience de la mesure prise.

Il n'est pas si clair que les étapes intermédiaires à une enquête policière quant à l'identification possible de suspects tombent sous le coup de la prohibition de l'usage d'outils biométriques sans le consentement de la personne concernée inscrite à la *Loi sur le cadre juridique des technologies de l'information*.

Il est par contre plus certain qu'un corps policier serait soumis à la divulgation obligatoire à la CAI d'une banque de données biométriques, même si elle doit servir dans un cadre autre que l'identification tel qu'entendu par la loi. En effet, l'article 45 soumet toute banque de données biométriques à la compétence de la Commission, que la banque soit ou non en service. Voici pourquoi la légalité de la règle 17 n'est pas non plus si évidente, puisqu'elle pourrait contredire les dispositions de la loi ou en modifier la portée par simple règle administrative.

### **7.3. Conclusion de l'analyse juridique des Règles d'utilisation de la vidéosurveillance**

L'analyse des pouvoirs réglementaires conférés par la LAI (voir section 6.1.6) nous a d'abord permis d'émettre certaines réserves d'ordre général quant à l'utilisation par la CAI de la technique de la directive administrative ou du guide pour encadrer le pouvoir discrétionnaire confié aux organismes publics en matière de protection des renseignements personnels et, *a fortiori*, tout pouvoir discrétionnaire confié à un organisme public pour s'acquitter de ses compétences propres.

---

La LAI accorde exclusivement au conseil des ministres le pouvoir d'encadrer par la voie réglementaire les mesures que doivent mettre en œuvre les organismes publics pour assurer la protection des renseignements personnels. La CAI ne peut donc pas faire par le biais d'une directive ce qui doit être déterminé par règlement du gouvernement.

Notre analyse plus détaillée du contenu des vingt règles sous étude nous permet de distinguer trois catégories de règles.

### 7.3.1. LES RÈGLES QUI REPRENENT AUTREMENT CE QUE DIT DÉJÀ LA LOI

On trouve d'abord une première catégorie des règles qui reprennent les prescriptions de la loi, mais en des termes différents mais encore larges, souvent mieux adaptés à la vidéosurveillance. Ces règles ont essentiellement une vocation pédagogique puisqu'elles ont pour objectif de préciser que ces principes tirés de la loi s'appliquent à la vidéosurveillance et éviter ainsi toute méprise de la part des organismes publics qui pourraient croire que les images colligées par les caméras ne sont pas des renseignements personnels au sens de la LAI. Ces règles ont une dimension plutôt pédagogique et de rappel auprès des organismes publics. On peut classer dans cette catégorie les règles 1, 6, 9, 10, 12 al. 1 et 3, 13, 14, 16, 18, 19 et 20. La validité de ces règles ne fait alors pas de doute.

On peut par ailleurs s'interroger sur leur utilité en matière d'opérationnalisation dans la mesure où elles relèvent davantage de la paraphrase des dispositions légales et ajoutent peu à l'encadrement susceptible de faciliter ou opérationnaliser l'application que doit en faire l'organisme et la surveillance qu'en fera la CAI.

### 7.3.2. LES RÈGLES QUI DEVRAIENT ÊTRE ÉDICTÉES PAR VOIE RÉGLEMENTAIRE ET QUI SONT DONC *ULTRA VIRES* DES POUVOIRS DE LA CAI

On peut identifier un autre groupe de règles qui soulèvent des questions sérieuses de validité juridique, dans la mesure où elles prévoient des normes que seul un règlement édicté par le gouvernement pourrait énoncer, selon la disposition habilitante de la loi, a. 63.2 LAI. On peut classer dans cette catégorie les règles 2, 3, 4, 5, 8, 11 et 12.

De plus, certaines de ces règles peuvent affecter de front le pouvoir discrétionnaire accordé par la loi qui régit l'organisme public, et notamment le large pouvoir discrétionnaire conféré aux autorités policières pour s'acquitter de leur mission de maintien de l'ordre, de prévention et de répression du crime et des infractions. Or, on sait qu'un pouvoir discrétionnaire conféré par la loi ne saurait être diminué par une simple règle administrative.

Une autre raison milite aussi fortement contre un pouvoir quasi-réglementaire poussé de la CAI pour préciser comment doivent être traduites les larges règles de la LAI

---

concernant la confidentialité, la finalité ou la nécessité de la collecte et de la gestion des renseignements personnels saisis par vidéosurveillance. Il s'agit du principe de justice naturelle *nemo iudex in sua causa*, le principe de l'impartialité.

La modulation du principe de l'impartialité qui doit animer tout pouvoir quasi-judiciaire s'applique autant à la fonction de surveillance et de contrôle qu'à la fonction juridictionnelle de la CAI. La DAE de la Commission exerce également une fonction quasi-judiciaire lorsqu'elle applique ses pouvoirs d'enquête aux systèmes de vidéosurveillance et émet des ordonnances pour rappeler à l'ordre les organismes publics qui contreviennent à la loi, aux règlements ou à ses vingt règles.

En raison de l'étendue et des précisions apportées par ces règles administratives, la CAI se retrouve dans la situation où elle doit porter un jugement et interpréter des règles qu'elle a elle-même énoncées. Or, en principe, nul «ne peut être enquêteur et arbitre dans la même affaire», à moins que la loi n'autorise le chevauchement de fonction<sup>84</sup>. On peut ici observer un certain chevauchement entre un pouvoir réglementaire (sous la forme de directives auxquelles une force quasi-réglementaire est accordée) et un pouvoir décisionnel, sous la forme d'émission d'ordonnance. Or, ce chevauchement n'est pas explicitement autorisé par la loi, puisque nous avons vu que la CAI outrepasserait vraisemblablement ses pouvoirs en utilisant la forme de la directive pour imposer des règles qui relèvent du pouvoir réglementaire du gouvernement.

Notre analyse nous permet de voir que la Commission a tenté de suppléer aux lacunes de la LAI en ce qui concerne le manque de précisions concernant la protection des renseignements personnels colligés par vidéosurveillance, en adoptant et mettant en application les *Règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*. Cette analyse nous indique par ailleurs que l'outil de la règle administrative utilisé jusqu'ici par la CAI pour tenter tant bien que mal un meilleur encadrement face au développement de la vidéosurveillance, paraît malheureusement mal adapté et inapproprié sinon, largement *ultra vires* des pouvoirs de la CAI. Cette observation devient encore plus pressante depuis l'adoption de l'article 63.2 LAI en 2006.

Ce sont les raisons pour lesquelles la simple révision de ces règles, comme le prévoyait le mandat original qui nous a été confié, n'offre pas de voie de solution valable pour la Commission.

Il est vrai que le pouvoir réglementaire de l'article 63.2 LAI n'a été ajouté à la loi qu'en 2006. Le gouvernement a adopté en 2008 un règlement en vertu de cette disposition

---

<sup>84</sup> Pierre Lemieux, *Droit administratif. Doctrine et jurisprudence*, 3<sup>e</sup> éd. Les Éditions Revue de droit de l'Université de Sherbrooke, 1998, p. 740.

---

habilitante. Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*<sup>85</sup> présente déjà une amorce de solution à un meilleur encadrement de la vidéosurveillance par les organismes publics. Nous allons nous y pencher à la section 8.

### 7.3.3. LES RÈGLES QUI CONTREDISENT UNE DISPOSITION DE LA LAI

Enfin, on trouve une troisième catégorie de règles qui pourraient contredire ou contrevenir directement à une disposition de la loi. Il s'agit sans doute de la catégorie qui pose le plus problème. Nous avons souligné que l'article de la loi qui introduit la règle de la transparence dans la collecte des renseignements personnels se trouve à l'article 65<sup>86</sup>.

On y prévoit notamment que la personne doit être informée lors de la cueillette du nom de l'organisme pour lequel le renseignement est colligé, des fins pour lesquelles il est recueilli, des catégories de personnes qui y auront accès ainsi que des droits d'accès et de rectification. Or, l'article 65 énonce à son alinéa 5 qu'il ne s'applique pas si le renseignement est recueilli pour des fins d'enquête ou de constat de faits par un organisme chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois.

Voilà pourquoi nous suggérons que les règles 7, 15 et 17 (en partie) contredisent la LAI et imposent des règles pour lesquelles la loi dispense les corps policiers, notamment.

---

<sup>85</sup> L.R.Q., c. A-2.1, r. 0.2.

<sup>86</sup> On trouve également des règles de transparence aux étapes subséquentes du traitement des renseignements, comme en matière de classement ou de communication des renseignements personnels.

---

## *8. Le pouvoir réglementaire du gouvernement quant aux mesures de protection des renseignements personnels*

Les vingt règles de la CAI tentaient tant bien que mal de suppléer au manque de précision du sens à donner aux principes généraux inscrits à la LAI dans le cadre de la vidéosurveillance. Ce type de limitation du pouvoir discrétionnaire relève davantage de l'ordre du règlement par opposition à la simple directive administrative. De plus, la CAI étant appelée à en vérifier l'application, il est dans le bon ordre des choses, afin de respecter le principe de l'impartialité, que les règles émanent du gouvernement et non pas de la CAI, ce que prévoit clairement la LAI depuis 2006.

Il apparaît donc que l'exercice du pouvoir réglementaire de la LAI par le conseil des ministres représente la meilleure voie pour encadrer correctement l'usage de la vidéosurveillance dans les lieux publics par les organismes publics.

### **8.1. Le règlement sur la diffusion de l'information et sur la protection des renseignements personnels**

#### 8.1.1. CHAMP D'APPLICATION DU RÈGLEMENT

Ce règlement adopté en 2006 s'appuie sur les deux nouvelles dispositions habilitantes de la LAI ajoutées au moment de l'adoption du projet de loi 86 en 2006 : l'article 63.2 LAI qui impose aux organismes publics assujettis de mettre en œuvre les mesures de protection des renseignements personnels prévues dans le règlement adopté par le gouvernement, ainsi que l'article 16.1 qui leur impose une diffusion sur internet des documents prescrits par règlement. Le nouveau règlement prévoit des règles de protection des renseignements personnels spécifiques aux systèmes de vidéosurveillance, confirmant ainsi que le gouvernement est bien conscient que ces systèmes de saisie de renseignements personnels en continu et à une échelle inédite pour les types de fichiers plus conventionnels, représentent un défi majeur nécessitant un encadrement mieux adapté aux menaces qu'ils représentent pour la protection des renseignements personnels et la vie privée. Un règlement du gouvernement du Québec, adapté à la vidéosurveillance représente une voie intéressante pour un meilleur usage des pouvoirs de contrôle de la CAI.

En optant de joindre dans un même règlement les nouvelles règles favorisant l'accès aux documents administratifs et celles devant promouvoir la protection des renseignements personnels, le gouvernement se devait en contrepartie de restreindre dans un premier temps le champ d'application du règlement, en le limitant aux organismes publics relevant directement du gouvernement. Les documents administratifs particuliers que détiennent les organismes décentralisés comme les

---

municipalités, les établissements de santé et de services sociaux ou encore le réseau de l'éducation exigeaient des règles mieux adaptées à leurs réalités avant de leur imposer une diffusion active de documents sur internet. C'est ainsi que l'article 1 du règlement précise ne pas s'appliquer aux organismes visés par les articles 5 (organismes municipaux), 6 (organismes scolaires) et 7 (établissements de santé et de services sociaux) de la LAI.

Or, ces organismes décentralisés sont sans doute ceux qui sont appelés à faire le plus grand usage des mécanismes de vidéosurveillance, si on exclut la surveillance des autoroutes et routes provinciales par le Ministère des Transports du Québec pour les contrôles d'excès de vitesse des véhicules moteurs ou autres infractions au Code de la route<sup>87</sup>, ou la sécurité de haltes routières<sup>88</sup>. En effet, outre les projets qui ont déjà fait l'objet d'une enquête de la CAI<sup>89</sup>, on apprend que l'installation de caméras de surveillance prend de l'ampleur dans les systèmes de transports en commun un peu partout à travers le Québec<sup>90</sup>, dont Montréal<sup>91</sup>, Québec<sup>92</sup> et Laval<sup>93</sup>.

---

<sup>87</sup> Transports Québec, «Radars photo et surveillance aux feux rouges — Québec dévoile les 15 endroits retenus dans le cadre de son projet pilote», Communiqué, 25 février 2009, en ligne : [www.RIMQ.qc.ca/news\\_detail.asp?ID=105940](http://www.RIMQ.qc.ca/news_detail.asp?ID=105940).

<sup>88</sup> Transports Québec, «Nouveau réseau de haltes routières en PPP — Signature d'une entente de partenariat», Communiqué, 4 novembre 2008, en ligne : [www.RIMQ.qc.ca/news\\_detail.asp?ID=100084](http://www.RIMQ.qc.ca/news_detail.asp?ID=100084).

<sup>89</sup> Le conseil municipal de la ville de Baie-Comeau a décidé lors de sa séance du 7 juillet 2008, de procéder à la vidéosurveillance de l'entrée de sa bibliothèque municipale. Ville de Baie-Comeau, «Vidéosurveillance à la Bibliothèque», Communiqué, 21 juillet 2008.

<sup>90</sup> Mais également pour la protection de d'autres types d'installations, comme les bâtiments et équipements municipaux, comme ceux dédiés à l'eau potable : Ville de Victoriaville, «Victoriaville — Projet de sécurisation des sources d'eau potable et des lieux publics», Communiqué, 18 mars 2009.

<sup>91</sup> J-L Fortin, «Des caméras dans les nouveaux autobus de la STM», *24 heures*, 26 janvier 2009. STM, «La STM lance son appel d'offres pour le remplacement des voitures de métro MR-63», Communiqué, 5 août 2008.

<sup>92</sup> Jean-François Néron, «Projet de caméras dans les autobus Les agressions physiques et verbales graves contre les chauffeurs ont triplé en un an », *Le Soleil*, 25 avril 2007.

<sup>93</sup> Hugo Morissette, «Pour contrer le vandalisme, des caméras seront installées dans les autobus de Laval», *24 heures*, 3 décembre 2008, p. 6.

---

### 8.1.2. ENCADREMENT DE LA VIDÉOSURVEILLANCE SELON LE RÈGLEMENT R. 0.2

Dans un guide de référence au Règlement<sup>94</sup> produit par la Direction de l'accès à l'information et de la protection des renseignements personnels (DAIPRP) du Secrétariat à la réforme des institutions démocratiques et à l'accès à l'information (SRIDAI), on mentionne que «tous les organismes publics soustraits ou exclus du Règlement [...] peuvent cependant appliquer, de façon volontaire, les règles qui y sont énoncées». On sait, par ailleurs, que cette situation hypothétique n'ouvre pas la voie à l'exercice des pouvoirs de surveillance de la CAI face à ses prescriptions.

Monsieur Robert Parent, directeur de la DAIPRP, nous a confirmé<sup>95</sup> que sa direction préparait actuellement un autre règlement pour assujettir les organismes exclus du Règlement r. 0.2.

Le modèle envisagé, présentement en discussion avec les fédérations municipales<sup>96</sup>, prévoit pour l'instant le même type d'encadrement de la vidéosurveillance par les organismes décentralisés que les modalités inscrites au Règlement A-2.1, r. 0.2. Il est donc important de s'attarder au modèle proposé.

Le modèle repose essentiellement sur la responsabilisation accrue des organismes publics en leur imposant la mise sur pied d'un comité interne relevant du dirigeant de l'organisme (a. 2, 2o)<sup>97</sup>, composé du responsable de l'accès à l'information et de la protection des renseignements personnels et, le cas échéant, du responsable de la sécurité de l'information et du responsable de la gestion documentaire. Ce comité peut s'adjoindre toute autre personne dont l'expertise est requise.

L'organisme public doit, dans le cas d'un système de vidéosurveillance :

- A. Aviser le comité du projet (a. 7, al. 1)
- B. Recevoir du comité les mesures particulières à respecter pour la protection des renseignements personnels, qui doivent comprendre au minimum six types de mesures (a. 7, al. 2) :
  - 1. la nomination d'une personne responsable
  - 2. l'évaluation des risques d'atteinte à la protection des renseignements personnels, dès l'étude préliminaire du projet

---

<sup>94</sup> Québec, *Guide de référence. Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*, mai 2008, 60 p.

<sup>95</sup> Conversation téléphonique du 10 mars 2009.

<sup>96</sup> UMQ (Union des Municipalités du Québec) et FQM (Fédération Québécoise des Municipalités).

<sup>97</sup> Et du sous-ministre, dans le cas d'un ministère.

- 
3. les mesures de protection des renseignements personnels pendant toute la période d'utilisation du système
  4. si le projet fait l'objet d'un contrat avec le secteur privé, l'inscription des exigences de protection des renseignements personnels à même le cahier de charges et le contrat
  5. la description des responsabilités des participants au projet
  6. la tenue d'activités de formation sur la protection des renseignements personnels à l'intention des participants au projet
- C. Recevoir du comité les mesures particulières en matière d'évaluation de la nécessité de recourir à la technologie de la vidéosurveillance (a. 9)
- D. Recevoir du comité les mesures particulières pour procéder à une évaluation (*audit*) de la conformité du système avec le droit à la vie privée
- E. Le dirigeant doit veiller à la sensibilisation et formation du personnel quant aux règles à suivre (a. 2, 3o)

Le comité interne doit, quant à lui :

- A. Fournir des mesures particulières pour les systèmes de vidéosurveillance qui doivent comprendre tous les points énoncés à l'article 7,
- B. Exiger de l'organisme selon une méthode prescrite par le comité interne, ou faire pour l'organisme selon cette méthode (le Règlement n'est pas clair) une évaluation de la nécessité de recourir à cette technologie et une évaluation de la conformité au droit au respect à la vie privée (a. 9).

Il appert du Règlement que le comité interne ne dispose que d'un pouvoir de recommandation auprès de la direction de l'organisme, qui demeure seule responsable de l'adoption du système et des mesures qu'il mettra en place. Puisque ce comité ne dispose d'aucune indépendance par rapport à la direction de l'organisme, on peut penser que les recommandations seront formulées en consensus avec la direction.

#### 8.1.3. OBSERVATIONS GÉNÉRALES SUR LE RÈGLEMENT R. 0.2

L'assujettissement des organismes publics à des mesures particulières et un suivi plus rigoureux à l'interne pour les systèmes de vidéosurveillance est un développement qui va dans la bonne direction. Nous avons observé dans notre analyse des pouvoirs dont dispose la CAI pour la surveillance des systèmes de vidéosurveillance qu'elle était mal outillée pour assurer le respect des normes de protection des renseignements personnels énoncées de façon trop large dans la LAI.

---

Il est opportun de faire reposer sur les organismes publics eux-mêmes les responsabilités de l'évaluation de la nécessité de la vidéosurveillance afin de mieux respecter leurs compétences propres en matière de prévention et de répression du crime et des infractions, par exemple.

Par ailleurs, on peut noter deux éléments qui mériteraient discussion.

La rédaction du Règlement ne nous donne aucune indication quant aux critères de l'évaluation de la nécessité de recourir à cette technologie, outre de dire que cette évaluation est nécessaire. On pourrait observer ici que cette obligation est déjà inscrite à la loi (a. 64 al. 1 LAI) et que le Règlement y ajoute peu, sauf pour introduire un intermédiaire sous la forme du comité interne, sans qu'il ne soit même clair si ce comité doit procéder lui-même à cette évaluation, ou simplement donner quelques indications à l'organisme quant à la façon de faire.

Une interprétation plus rationnelle du Règlement, de façon à lui donner un effet, serait de soutenir que les deux mesures de l'article 9 s'ajoutent, dans le cas de la vidéosurveillance aux 6 mesures de l'article 7, et que donc, c'est le comité interne qui doit procéder à l'évaluation de la nécessité du système et à son audit après sa mise en place. Mais, même avec cette interprétation, le règlement ne donne aucune indication au comité interne quant à ce qui doit être pris en compte ou précisé.

La CAI se retrouverait alors dans la même situation de flou juridique face aux systèmes de vidéosurveillance, pour faire appliquer et respecter les grands principes de la LAI en matière de protection des renseignements personnels, et particulièrement pour le principe de la nécessité.

La deuxième observation importante à faire concernant le Règlement r. 0.2 concerne l'absence de toute mesure de transparence quant au système de vidéosurveillance. Nous avons souligné à la section 7.2.2, lorsque nous avons étudié les règles 7 et 15 de la CAI, que l'article 65 LAI ne s'applique pas «à une enquête ou à un constat faits par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois». Nous avons alors souligné que même si les règles 7 et 15 de la CAI ne pouvaient pas s'appuyer sur la loi, il serait sans doute opportun de repenser cette situation, puisque le législateur n'avait sans doute pas en tête le type de collecte de données en continu et sur une base potentiellement massive comme peut le faire la vidéosurveillance, lorsqu'il a prévu l'exclusion de l'assujettissement des corps policiers, municipaux ou de la Sûreté du Québec à cette règle de transparence. La discussion d'un nouveau règlement pour l'assujettissement des organismes publics décentralisés devrait être l'occasion de débattre et repenser cette règle qui semble si mal adaptée au respect de la vie privée par ces systèmes, qu'entend pourtant faire valoir le règlement. En effet, le règlement impose une évaluation en termes encore plus

---

larges que la LAI, puisque l'évaluation doit porter, selon l'article 9, 2o, non seulement sur la protection des renseignements personnels, mais sur le respect de la vie privée.

On peut craindre que la formulation au Règlement r. 0.2 des responsabilités respectives du comité interne et de la direction de l'organisme n'apporte que peu d'aide aux pouvoirs de contrôle et de surveillance de la CAI, outre la vérification de la mise sur pied du comité interne et de la transmission et réception de mesures formelles de protection, dont la forme et le contenu sont très peu encadrés au-delà de ce que prévoit déjà la LAI. On aurait pu s'attendre à ce que l'exercice du pouvoir réglementaire du gouvernement permette un encadrement plus serré du pouvoir discrétionnaire des organismes publics de juger des mesures de protection, et notamment dans le contexte de la vidéosurveillance.

Les leçons tirées de notre analyse nous indiquent que les règles qui devraient être incluses dans un règlement concernant surtout les mesures qui doivent être adoptées avant même la décision d'installation de caméras de surveillance, comme le démontrent les trois projets qui ont fait l'objet d'une inspection et d'une analyse de la CAI, dont les lacunes sont le plus souvent responsables des principaux manquements en matière de protection des renseignements personnels.

#### 8.1.4. SUGGESTION POUR UNE MEILLEURE ÉVALUATION DU RÈGLEMENT R.0.2

Tous les organismes publics, à l'exception des organismes décentralisés mentionnés ci-haut, sont déjà soumis aux prescriptions du Règlement r.0.2 depuis le 29 mai 2008. Or, certains projets de vidéosurveillance sont déjà lancés par des ministères, dont Transports Québec. La signature d'un contrat de PPP a été annoncée le 4 novembre 2008 pour la construction de sept haltes routières à travers le Québec, qui doivent être munies de caméras de vidéosurveillance.

Le 25 février dernier la ministre des Transports du Québec annonçait que des caméras de vidéosurveillance seraient installées à quinze endroits différents (Montréal, Montérégie et Chaudières-Appalaches) pour prendre des photos radars aux feux rouges afin de vérifier le respect du Code de la sécurité routière<sup>98</sup>.

---

<sup>98</sup> Certains règlements et arrêtés ministériels ont été publiés le 29 avril dernier pour préciser les modalités d'inspection de ces appareils (*Règlement sur les conditions et les modalités d'utilisation des cinémomètres photographiques et des systèmes photographiques de contrôle de la circulation aux feux rouges*, R.R.Q., c. C-24.2, r. 0.1.0002), ou les endroits d'installation et le type de mesure prise par les appareils, soit la vitesse ou le respect du feu rouge (*Arrêté ministériel concernant les endroits où peuvent être utilisés les cinémomètres photographiques fixes*, R.R.Q., c. C-24.2, r. 0.1.02.1; *Arrêté ministériel concernant les endroits où peuvent être utilisés les cinémomètres photographiques mobiles*, R.R.Q., c. C-24.2, r. 0.1.02.2; *Arrêté ministériel concernant les endroits où peuvent être utilisés les systèmes photographiques de contrôle de circulation aux feux rouges*, R.R.Q., c. C-24.2, r. 0.1.02.3).

---

Il serait donc très pertinent de procéder à une analyse, dans le cadre de ces projets ou d'autres à identifier, pour déterminer si le Règlement r.0.2 est connu de Transports Québec ou des autres ministères, comment il est appliqué et interprété et quels en sont les effets réels quant à la l'implantation de mesures de protection des renseignements personnels.

Cette analyse serait fort utile pour mieux préparer le Règlement en gestation pour les organismes décentralisés.

## **8.2. La participation de la CAI à la réflexion menant à la préparation d'un nouveau règlement**

La LAI prévoit à son article 123 que la CAI doit donner son avis sur tout projet de règlement adopté en vertu de la LAI.

On sait qu'un projet (qui pourrait prendre la forme de plus d'un règlement, ou d'un amendement au Règlement r.0.2, ou encore, une combinaison de ces deux possibilités) est déjà en gestion à la DAIPRP concernant l'assujettissement des organismes exclus du Règlement r.0.2. Pendant que les fédérations municipales sont déjà impliquées dans un processus de consultation, la CAI est, pour l'instant, tenue à l'écart. Or, non seulement la CAI est au premier rang des intéressés par le règlement, mais surtout, elle dispose d'une expérience de plusieurs années quant aux questions soulevées par le respect des mesures de protection de renseignements personnels par les systèmes de vidéosurveillance, dont ne peut ainsi profiter la DAIPRP.

Est-il plausible que la DAIPRP pense qu'elle peut compter sur la présence des vingt Règles de la CAI pour compléter les dispositions vagues du Règlement r. 0.2? La même approche prévaudra-t-elle pour les autres règlements actuellement en gestation? Or, nous avons vu que non seulement les Règles de la CAI ne peuvent pas pallier aux imprécisions d'un règlement du gouvernement, mais que certaines de ces règles devraient plutôt être intégrées à même un tel règlement pour en assurer l'application.

Il est pertinent de noter que les règles qui devraient être édictées par règlement, soit les règles 1, 2, 3, 4 et 5 sont justement celles qui ont fait l'objet d'une conclusion plus sévère au niveau des manquements des projets des villes de Baie-Comeau, Sherbrooke et Montréal. Or, le règlement r.0.2 ne fournit aucun encadrement par rapport à ce type de normes

Au surplus, en ce qui concerne le principe de la transparence, des amendements à la loi seraient nécessaires pour permettre un meilleur arrimage des compétences et pouvoirs de la CAI et des organismes soumis à son pouvoir de surveillance.



Bref, il serait sans doute important que la CAI participe de façon plus hâtive que tardive aux réflexions concernant la préparation du Règlement visant à assujettir les organismes publics décentralisés à des mesures mieux adaptées à la vidéosurveillance.

---

## 9. Conclusion

Une deuxième révision des règles de la CAI quant à l'utilisation de la vidéosurveillance dans les lieux publics par les organismes publics (c'est-à-dire l'actuel document *Les règles d'utilisation de la vidéosurveillance avec enregistrement dans les lieux publics par les organismes publics*, adopté par la CAI et publié en juin 2004), ne représente pas la voie de solution aux difficultés que rencontre la CAI à faire respecter les principes de la protection des renseignements personnels énoncés dans la LAI, par les organismes publics qui s'adonnent à la vidéosurveillance des lieux publics au Québec.

Si la CAI a choisi d'adopter ce type de directives ou de guide en 2002 (adoption) et 2004 (première révision), c'est qu'elle estimait, avec raison, que les organismes publics éprouvaient des difficultés à saisir ce qu'exige le respect des principes de confidentialité, de sécurité, de nécessité, de transparence et de finalité dans le cadre de l'utilisation de la vidéosurveillance et de l'enregistrement des images. Cette situation était également susceptible d'engendrer des variations importantes quant à l'interprétation des principes de la loi selon les organismes ou les projets de vidéosurveillance, ce qui pose problème en termes d'égalité de tous devant la loi.

On peut conclure aujourd'hui que la LAI présentait alors des déficiences importantes puisque les principes inscrits à la loi ne faisaient l'objet d'aucunes précisions opérationnelles. On sait que «la loi ne contient souvent que des dispositions qui forment un cadre très général sans déterminer d'orientations précises» et c'est la raison pour laquelle, «c'est à la lecture des règlements valablement adoptés que l'on retrouvera paradoxalement le cadre plus précis relativement à la finalité de la loi»<sup>99</sup>. Le règlement est un complément nécessaire de la loi, dans la mesure où il permet d'énoncer les détails plus techniques ou administratifs qui doivent traduire sur le terrain le respect des principes généraux de la loi.

La LAI n'offrait alors aucun pouvoir réglementaire pour encadrer les principes généraux de la loi avant sa modification en 2006. C'est en ce sens que la CAI a dû se substituer à ce rôle en adoptant en 2004 les directives en vingt règles. Tout en visant la résolution d'un problème, cette substitution posait plusieurs problèmes.

D'abord, la révision poussée de la CAI des méthodes policières de prévention du crime heurte de front le large pouvoir discrétionnaire dont bénéficient les corps policiers pour répondre de leur compétence propre en matière de maintien de la paix, de l'ordre et de la sécurité publique (*Loi sur la police*) ainsi que le pouvoir discrétionnaire des municipalités concernant les mesures de sécurité civile (*Loi sur les compétences municipales*). Or, le principe de la hiérarchie des normes nous enseigne que la simple

---

<sup>99</sup> Pierre Issalys, Denis Lemieux, id. p.72-73.

---

directive administrative ne peut prévaloir ou restreindre un pouvoir discrétionnaire conféré par la loi.

Cette situation pouvait également générer chez une personne raisonnable la crainte que la règle de l'impartialité de l'exercice des pouvoirs de la CAI ne soit pas respectée, puisque le même organisme édicte des règles qu'il est ensuite appelé à faire respecter par le biais de ses pouvoirs d'enquête et d'ordonnance. Bref, même si la CAI était justifiée de prendre des mesures pour assurer un meilleur respect de la loi, le seul mécanisme qui s'offrait alors à elle de la directive administrative équivalant à un pouvoir quasi-réglementaire plaçait la CAI dans une situation aussi difficile que précaire sur le plan du droit et de l'opération.

L'amendement à la loi de 2006 qui a ajouté l'article 63.2 LAI, qui prévoit un pouvoir réglementaire exclusif du gouvernement du Québec pour préciser les mesures à prendre pour protéger les renseignements personnels, change quelque peu l'analyse juridique de la situation. La CAI n'est, depuis, plus habilitée [si on estime qu'elle l'a déjà été] à se substituer au gouvernement dans l'exercice d'un pouvoir réglementaire ou quasi-réglementaire. Cette situation invalide donc indirectement les règles qui visent à encadrer de façon plus précise les principes généraux de la loi. Au surplus, on peut interpréter l'article 65 de la loi comme exemptant les organismes chargés de prévenir et réprimer le crime de certaines obligations en matière de transparence, que contredisent certaines des règles adoptées par la Commission.

Notre analyse plus détaillée des vingt règles confirme cette appréhension et nous permet de conclure que la seule voie de solution pour mieux encadrer les systèmes de vidéosurveillance repose sur un règlement du gouvernement du Québec qui s'appuie sur les enseignements tirés de l'expérience de la surveillance de la Commission de ces systèmes.

Le Règlement du gouvernement adopté en 2008 présente une approche intéressante de responsabilisation des organismes publics, chargés de mettre en place un comité conseil interne responsable de mesures précises de protection des renseignements personnels. Par contre, le règlement ne donne malheureusement aucune indication plus précise que ne le prévoit déjà la loi, notamment en matière d'évaluation de la nécessité de recourir à la technologie de la vidéosurveillance, qui, selon l'expérience de la CAI, présente toujours une difficulté importante dans l'analyse de ces systèmes.

Le Règlement est en vigueur depuis le 29 mai 2008, et déjà certains ministères assujettis ont lancé des projets de vidéosurveillance, sans que l'on sache si le Règlement aura réussi à induire une plus grande responsabilisation de ces ministères (notamment Transports Québec) par rapport à leurs responsabilités en matière de protection des renseignements personnels. Nous suggérons qu'une analyse de l'effet du Règlement soit entamée rapidement, en collaboration avec la DAIPRP, au moment où

---

cette direction prépare déjà un autre Règlement pour l'assujettissement des organismes publics décentralisés, dont les organismes municipaux. Afin d'assurer une meilleure gestion de ces dossiers, tant par les organismes publics responsables en premier lieu du respect des principes de protection des renseignements personnels, que des fonctions de surveillance et de contrôle que la loi confie à la CAI, la Commission devrait être associée au plus tôt à la démarche de préparation d'un nouveau règlement, afin de son expertise sur la matière soit mise à contribution dans le meilleur intérêt de tous.