Commissaire à
l'information et à
la protection de la
vie privée de l'Ontario

Lignes directrices sur l'utilisation de caméras de surveillance vidéo dans les endroits publics

Ann Cavoukian, Ph.D.
Commissaire
Septembre 2007

Remerciements

Le présent document est une mise à jour de la version publiée en 2001 par Ann Cavoukian, Ph.D., commissaire à l'information et à la protection de la vie privée de l'Ontario. M^me^ Cavoukian tient à souligner la participation de Judith Hoffman à la préparation du premier rapport, et de Catherine Thompson à celle de la présente version.

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
CANADA
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site web : www.ipc.on.ca

Table des matières

1. Introduction

Les institutions gouvernementales envisagent de plus en plus la mise en œuvre de technologies de surveillance vidéo dans le cadre des programmes d'application de la loi et de sécurité publique. Dans des circonstances limitées et précises, les caméras de surveillance vidéo peuvent effectivement permettre de protéger la sécurité publique, de déceler les actes criminels et de contribuer aux enquêtes à leur sujet, en plus d'avoir un effet dissuasif.

Il est recommandé aux institutions régies par la *Loi sur l'accès à l'information et la protection de la vie privée* (la *Loi* provinciale) et la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (la *Loi* municipale) de ne pas considérer les programmes de surveillance vidéo comme une panacée. Les solutions technologiques aux problèmes de sécurité s'appuient sur un souci de justice et de sécurité absolues, pour tous et en toutes circonstances[1], mais une telle perfection est irréaliste. Les institutions doivent établir un équilibre entre les avantages de la surveillance vidéo pour le public et le droit des particuliers de ne pas subir une atteinte injustifiée à leur vie privée. Or, la surveillance généralisée et sans motif apparent des activités publiques courantes et légales porte atteinte à la vie privée.

Les présentes lignes directrices ont pour but d'aider les institutions à déterminer si la collecte de renseignements personnels au moyen d'un système de surveillance vidéo est légale et justifiable et, le cas échéant, d'expliquer comment intégrer des mesures de protection de la vie privée dans pareil système.

Ces lignes directrices ne s'appliquent pas à la surveillance secrète ou à la surveillance en tant qu'outil d'enquête utilisé dans des cas précis pour l'application de la loi, lorsque la loi ou un mandat de perquisition l'autorise.

Elles ne s'appliquent pas non plus aux systèmes utilisés aux fins de la surveillance du personnel dans les lieux de travail.

[1] À ce sujet, voir Jeffrey Rosen, *The Naked Crowd: Reclaiming Security and Freedom in an Anxious Age*, Toronto, Random House, 2004, page 123. Voir également le chapitre 3 de cet ouvrage, « Silver Bullet ».

2. Définitions

Les définitions suivantes s'appliquent aux présentes lignes directrices.

Renseignements personnels, aux termes de l'article 2 des *Lois*, désigne des renseignements consignés ayant trait à un particulier qui peut être identifié. S'entend notamment des renseignements concernant la race, la couleur, l'origine nationale ou ethnique, le sexe et l'âge. Si un système de surveillance vidéo consigne ces caractéristiques d'un particulier qui peut être identifié ou les activités auxquelles il se livre, les enregistrements seront considérés comme des « renseignements personnels » au sens des *Lois*.

Document, également aux termes de l'article 2 des *Lois*, désigne un document qui reproduit des renseignements sans égard à leur mode de transcription, que ce soit sous forme imprimée, sur film, au moyen de dispositifs électroniques ou autrement. S'entend notamment des photographies, films, microfilms, bandes magnétoscopiques, documents lisibles par machine et documents produits à partir de documents lisibles par machine.

Système de surveillance vidéo désigne un système ou un dispositif mécanique, électronique, numérique ou sans fil[2] de surveillance qui permet l'enregistrement, l'observation ou le contrôle vidéo continu ou périodique de renseignements personnels sur des particuliers dans des endroits accessibles au public (y compris des rues, routes et parcs). Dans les présentes lignes directrices, ce terme s'applique aux appareils audio, aux technologies d'imagerie thermique ou à tout autre dispositif permettant de produire une image d'un particulier.

Matériel de réception désigne le matériel ou le dispositif employé pour recevoir ou enregistrer les renseignements personnels recueillis au moyen d'un système de surveillance vidéo, comme une caméra, un moniteur ou tout autre appareil vidéo, audio, mécanique, électronique ou numérique.

Dispositif de stockage désigne une bande vidéo, un disque rigide d'ordinateur, un cédérom, une puce électronique ou tout autre appareil utilisé pour stocker les données, les images ou les sons captés par un système de surveillance vidéo.

[2] Voir la feuille-info *Technologies de communication sans fil : les systèmes de surveillance vidéo* sur le site du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (www.ipc.on.ca).

3. Collecte de renseignements personnels au moyen d'un système de surveillance vidéo

Les données, les images et les sons d'un particulier qui peut être identifié représentent des « renseignements personnels » aux termes des *Lois*[3].

Étant donné que les systèmes de surveillance vidéo peuvent servir à recueillir des renseignements personnels sur des particuliers pouvant être identifiés, les institutions doivent déterminer si elles ont le pouvoir de recueillir ces renseignements en vertu des *Lois*.

Aux termes du paragraphe 38 (2) de la *Loi* provinciale et du paragraphe 28 (2) de la *Loi* municipale, nul ne doit recueillir des renseignements personnels pour le compte d'une institution à moins d'y être autorisé expressément par une loi, ou à moins que ces renseignements servent à l'exécution de la loi ou soient nécessaires au bon exercice d'une activité autorisée par la loi. Par exemple, la collecte de renseignements personnels uniquement pour des raisons pratiques, sans que cela ne soit nécessaire au bon exercice d'une activité autorisée par la loi, ne serait pas acceptable aux termes des paragraphes 28 (2) et 38 (2)[4].

Les institutions doivent être en mesure de démontrer que toute collecte actuelle ou proposée de renseignements personnels au moyen d'un système de surveillance vidéo est autorisée en vertu de ces dispositions.

[3] Soulignons qu'en vertu d'une ordonnance du CIPVP, un document est créé lorsqu'une caméra capte une image, l'encode et la transmet sans fil, même si aucun support physique comme une bande vidéo ou un cédérom n'est créé, aux termes de la *Loi sur la protection des renseignements personnels sur la santé*. Voir l'ordonnance HO-005 sur le site Web du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (www.ipc.on.ca).

[4] *Cash Converters Canada Inc. v. Oshawa* (City) [2007] O.J. No. 2613, 40.

4. Facteurs à envisager avant d'utiliser un système de surveillance vidéo

Avant de recourir à un système de surveillance vidéo, il est recommandé aux institutions de suivre les critères suivants :

- L'utilisation d'un système de surveillance vidéo ne devrait être envisagée que si le recours à d'autres mesures de protection de la sécurité publique, de dissuasion, de dépistage ou d'aide au processus d'enquête sur des actes criminels a été jugé impossible.

  La surveillance vidéo ne devrait être employée que dans les cas où des techniques conventionnelles (p. ex., patrouilles pédestres) ne peuvent être employées dans les circonstances ou sont beaucoup moins efficaces que la surveillance pour appliquer la loi ou assurer la sécurité publique, et lorsque les avantages de la surveillance l'emportent sur l'atteinte à la vie privée que comporte la collecte de renseignements personnels au moyen d'un système de surveillance vidéo.

- L'utilisation de chaque caméra de surveillance devrait être justifiée par des rapports précis et vérifiables d'actes criminels ou d'inquiétudes importantes en matière de sécurité.

- L'incidence que pourrait avoir le système proposé de surveillance vidéo sur la vie privée et les moyens d'en réduire les effets négatifs devraient être évalués en examinant les modalités de collecte, d'utilisation, de divulgation et de conservation des renseignements personnels. Les institutions pourraient consulter à ce sujet l'outil d'évaluation de l'incidence sur la vie privée du gouvernement de l'Ontario[5].

- Des consultations devraient avoir lieu avec les intervenants pertinents pour discuter de la nécessité du programme proposé de surveillance vidéo et déterminer si le public le considère comme acceptable. Il y a lieu également de mener des consultations publiques intensives.

- Les institutions doivent s'assurer que le système de surveillance vidéo est conçu et utilisé de façon à réduire l'atteinte à la vie privée au minimum nécessaire pour réaliser les objectifs légaux fixés.

[5] Accessible (en anglais seulement) à http://www.accessandprivacy.gov.on.ca/english/pub/screeningtool.html.

5. Élaboration d'une politique concernant un système de surveillance vidéo

Après avoir décidé d'utiliser un système de surveillance vidéo, l'institution devrait élaborer et mettre en œuvre une politique exhaustive concernant son fonctionnement. Cette politique devrait comprendre les aspects suivants :

- La raison d'être et les objectifs du système de surveillance vidéo.
- L'utilisation du système, y compris l'emplacement du matériel de réception, le personnel autorisé à s'en servir et à accéder au matériel de stockage et les périodes de surveillance.
- Les obligations de l'institution concernant les avis ainsi que l'accès aux documents, leur utilisation, leur divulgation, leur conservation, leur destruction et les aspects touchant la sécurité conformément aux *Lois* (voir la section 7).
- Le cadre supérieur désigné responsable du respect des obligations de l'institution à l'égard de la vie privée en vertu des *Lois* et de sa politique.
- Une règle selon laquelle l'institution conservera le contrôle et la responsabilité du système de surveillance vidéo en tout temps.
- Une règle selon laquelle toute entente entre l'institution et les fournisseurs de services doit préciser que l'institution a le contrôle des documents traités ou créés dans le cadre de la prestation de services de surveillance vidéo et que ces documents sont assujettis aux *Lois*.
- Une règle selon laquelle le personnel et les fournisseurs de services doivent se familiariser avec la politique et les *Lois* et s'y conformer dans l'exercice de leurs fonctions et obligations relativement à l'utilisation du système de surveillance vidéo.

  Les employés qui enfreignent la politique ou les dispositions des *Lois* ou d'autres lois pertinentes devraient être passibles de mesures disciplinaires. Dans le cas d'un fournisseur de services, pareil manquement serait considéré comme une rupture de contrat donnant lieu à des sanctions pouvant aller jusqu'à la résiliation du contrat.

  Les employés des institutions et des fournisseurs de services devraient signer une entente concernant leurs obligations en vertu de la politique et des *Lois* et les engageant à préserver le caractère confidentiel des renseignements.

- Une règle selon laquelle un processus est établi en cas de divulgation accidentelle de renseignements personnels[6].

- L'intégration de la politique dans les programmes de formation et d'orientation de l'institution et des fournisseurs de services. Une formation périodique devrait être fournie sur les obligations du personnel aux termes des *Lois*.
- L'examen et la mise à jour de la politique tous les deux ans ou plus souvent en cas de modification ou de mise à niveau du système de surveillance vidéo.

[6] Il y a atteinte à la vie privée lorsque des renseignements personnels sont recueillis, conservés, utilisés ou divulgués d'une façon qui n'est pas conforme aux dispositions des *Lois*. Voir les publications accessibles sur le site du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (www.ipc.on.ca), comme *Outil d'évaluation aux fins de la notification en cas d'atteinte à la vie privée et Que faire en cas d'atteinte à la vie privée : Lignes directrices pour les organismes gouvernementaux*.

6. Conception et installation du matériel de surveillance vidéo

L'institution devrait envisager les aspects suivants relativement à la conception d'un système de surveillance vidéo et à l'installation du matériel :

- Le matériel de réception comme les caméras vidéo et les dispositifs audio et autres devraient être installés uniquement dans des endroits publics désignés, où la surveillance vidéo est nécessaire pour protéger la sécurité publique, à des fins de dépistage ou de dissuasion ou pour contribuer aux enquêtes sur des actes criminels.

- Le matériel doit être installé de façon à ne permettre la surveillance que des endroits où celle-ci a été considérée comme nécessaire. Les caméras ne doivent pas être orientées vers les fenêtres des immeubles adjacents.

- Si les caméras sont réglables, les réglages devraient être limités dans la mesure du possible afin que les opérateurs ne puissent les régler, faire un zoom ou les manipuler pour surveiller des endroits qui ne sont pas visés par le programme de surveillance vidéo.

- Le matériel ne doit jamais servir à surveiller des endroits où le public et le personnel ont des attentes élevées en matière de vie privée (p. ex., vestiaires et salles de bain).

- L'institution devrait envisager d'utiliser le système de surveillance vidéo uniquement pendant les périodes où la probabilité que des actes criminels soient commis et décelés dans les endroits sous surveillance est manifestement élevée.

- Le public devrait être informé de la surveillance au moyen d'affiches claires apposées à des endroits visibles au périmètre de la zone surveillée, en guise d'avertissement. Ces affiches devraient donner le nom d'une personne à qui s'adresser pour obtenir des renseignements sur le système de surveillance vidéo, avec son adresse, son numéro de téléphone ou son site Web.

- En outre, en vertu du paragraphe 39 (2) de la *Loi* provinciale et du paragraphe 29 (2) de la *Loi* municipale, les particuliers doivent être informés de l'autorité légale invoquée pour justifier la collecte de renseignements personnels, des fins principales auxquelles ces renseignements doivent servir ainsi que des titre, adresse et numéro de téléphone d'affaires d'une personne qui peut renseigner les particuliers au sujet de cette collecte. Ces renseignements peuvent être inscrits sur des affiches ou fournis par d'autres moyens, notamment la distribution de dépliants ou sur le site Web de l'institution. Voir un exemple d'affiche municipale à l'annexe A.

- Les institutions devraient faire preuve de la plus grande transparence au sujet du programme de surveillance vidéo et, sur demande, fournir au public la raison d'être de ce programme, ses objectifs et les politiques et procédures établies. Elles peuvent le faire au moyen d'un dépliant ou d'un livret, ou encore afficher une description du programme sur leur site Web.

- Le matériel de réception devrait être installé dans un bureau à accès strictement contrôlé. Seul le personnel responsable ou les personnes ayant reçu l'autorisation écrite de ce personnel conformément à la politique de l'institution devraient avoir accès à ce bureau et au matériel de réception. Les moniteurs doivent être placés hors de la vue du public.

7. Accès aux documents de surveillance vidéo et utilisation, divulgation, conservation, sécurité et destruction de ces documents

Les renseignements obtenus au moyen d'un système de surveillance vidéo ne doivent servir qu'aux fins établies dans la raison d'être et les objectifs du programme de surveillance, qu'il s'agisse de protéger la sécurité publique, de déceler les actes criminels, d'avoir un effet dissuasif ou de contribuer aux enquêtes sur de tels actes. Ces renseignements ne doivent pas être conservés ou utilisés à d'autres fins.

L'institution qui compte conserver des documents créés par surveillance vidéo et contenant des renseignements personnels doit instaurer les politiques et procédures suivantes et les inclure dans sa politique décrite à la section 5 :

- Les bandes magnétiques et autres dispositifs de stockage doivent être placés après usage dans un contenant verrouillé se trouvant dans un bureau à accès contrôlé. Chaque dispositif doit porter la date et un numéro séquentiel unique ou un autre symbole vérifiable.

- L'accès aux dispositifs de stockage doit être réservé au personnel autorisé. Les accès et utilisations des enregistrements doivent être consignés dans un journal afin de permettre leur vérification. Les journaux électroniques doivent être conservés là où le sont les documents électroniques.

- L'institution doit élaborer des politiques écrites sur l'utilisation et la conservation des renseignements consignés. Ces politiques doivent notamment :

    ° préciser clairement qui peut consulter les renseignements et les circonstances dans lesquelles cette consultation est autorisée (p. ex., parce qu'un incident a été signalé, ou pour enquêter sur un crime éventuel);

    ° établir la période de conservation des renseignements qui n'ont pas été consultés à des fins d'application de la loi ou de sécurité publique. Les renseignements consignés qui n'ont pas été utilisés à ces fins doivent être détruits selon un calendrier établi (normalement de 48 à 72 heures plus tard). Par exemple, les images que capte un système de surveillance vidéo installé en 2007 dans le quartier du divertissement de Toronto ne sont pas examinées. Elles sont effacées automatiquement après 72 heures et on n'y accède qu'en cas d'incident qui motive une enquête;

    ° établir une période de conservation distincte pour les renseignements consignés qui ont été consultés à des fins d'application de la loi ou de sécurité publique. En vertu du paragraphe 5 (1) du Règlement de l'Ontario 460 pris en application de la *Loi* provinciale,

ces renseignements doivent être conservés pendant un an. Bien que l'article 5 du Règlement de l'Ontario 823 pris en application de la *Loi* municipale contienne une disposition semblable, une institution municipale peut raccourcir la période de conservation par voie de résolution ou de règlement.

- Les institutions municipales devraient envisager d'adopter un règlement ou une résolution, comme le prévoit l'article 5 du Règlement de l'Ontario 823, pour établir clairement leur calendrier de conservation.

- L'institution doit conserver les dispositifs de stockage contenant des éléments de preuve en suivant les procédures normales jusqu'à ce que les autorités en fassent la demande. Avant de remettre un dispositif de stockage aux autorités, une formule d'autorisation devrait être remplie. Cette formule devrait indiquer qui a pris le dispositif et sous quelle autorité de même que la date de la remise, et préciser si le dispositif sera renvoyé ou détruit après usage. Cette procédure doit être surveillée régulièrement et strictement appliquée.

- Les vieux dispositifs de stockage doivent être détruits de façon sécuritaire, afin que les renseignements personnels qu'ils contiennent ne puissent être récupérés ou reconstitués. Parmi les méthodes de destruction, mentionnons le déchiquetage, l'incinération ou l'effacement magnétique. Voir la feuille-info *La destruction sécurisée de renseignements personnels* sur le site Web du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (www.ipc.on.ca).

- En vertu de l'article 47 de la *Loi* provinciale et de l'article 36 de la *Loi* municipale, tout particulier a un droit d'accès aux renseignements personnels qui le concernent qui ont été recueillis au moyen d'un système de surveillance vidéo. Les politiques et procédures établies doivent en tenir compte. L'accès à une partie ou à la totalité des renseignements personnels peut être accordé, à moins qu'une exception ne s'applique en vertu de l'article 49 de la *Loi* provinciale ou de l'article 38 de la *Loi* municipale qui ferait en sorte que la divulgation représenterait une atteinte injustifiée à la vie privée d'un autre particulier. Dans ce cas, l'accès aux renseignements personnels peut reposer également sur la possibilité de retirer du document les renseignements qui font l'objet de l'exception. On peut le faire notamment en « noircissant » de façon numérique les images d'autres personnes que l'on peut voir sur les bandes vidéo.

Les systèmes de surveillance vidéo qui utilisent une technologie sans fil doivent chiffrer de façon sécurisée les transmissions de renseignements personnels. À ce sujet, voir la feuille-info *Technologies de communication sans fil : Protection de la vie privée et sécurité* sur le site du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (www.ipc.on.ca).

8. Vérification et évaluation de l'utilisation d'un système de surveillance vidéo

Les institutions devraient soumettre à des vérifications régulières l'utilisation et la sécurité du matériel de surveillance vidéo. Cette tâche, qui pourrait être confiée à un vérificateur externe, devrait également porter sur la conformité de l'institution aux politiques et procédures opérationnelles. Les lacunes relevées lors d'une vérification doivent être comblées immédiatement.

Le personnel et les fournisseurs de services devraient être informés du fait que leurs activités seront vérifiées, et qu'ils pourraient être appelés à justifier pourquoi telle ou telle personne devrait, à leur avis, faire l'objet d'une surveillance.

L'institution devrait examiner et évaluer régulièrement son programme de surveillance vidéo pour déterminer s'il demeure justifié conformément aux exigences de la section 4. Cette évaluation devrait avoir lieu au moins une fois par année.

9. Autres ressources

Les renseignements personnels recueillis au moyen du système de surveillance vidéo d'une institution ainsi que les politiques et pratiques de cette institution relativement à ces renseignements sont assujettis aux dispositions des *Lois* concernant la protection de la vie privée.

Avant d'installer un système de surveillance vidéo ou de mettre en œuvre tout autre programme pouvant avoir une incidence sur la vie privée, les institutions devraient obtenir des conseils juridiques et consulter leur coordonnatrice ou coordonnateur de l'accès à l'information et de la protection de la vie privée. Les coordonnatrices et coordonnateurs peuvent consulter le Bureau de l'accès à l'information et de la protection de la vie privée du ministère des Services gouvernementaux et des Services aux consommateurs.

Le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario veille au respect des dispositions des *Lois* en matière de protection de la vie privée. Les institutions qui ont l'intention d'implanter, de modifier de façon importante ou d'élargir la portée d'un système de surveillance vidéo devraient le consulter au préalable.

Les institutions devraient également consulter les publications suivantes, accessibles sur le site Web du Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (www.ipc.on.ca) :

- *Technologies de communication sans fil : Protection de la vie privée et sécurité* (feuille-info)
- *Technologies de communication sans fil : les systèmes de surveillance vidéo* (feuille-info)
- *La destruction sécurisée de renseignements personnels* (feuille-info)
- *Outil d'évaluation aux fins de la notification en cas d'atteinte à la vie privée*
- *Que faire en cas d'atteinte à la vie privée : Lignes directrices pour les organismes gouvernementaux*

Annexe A – Exemple d'avis municipal

Attention

Ce secteur est surveillé au moyen de caméras vidéo

Des renseignements personnels sont ainsi recueillis en vertu de la (loi) et du (règlement municipal). Ils seront utilisés pour protéger la sécurité publique et réduire la criminalité dans ce secteur.

Les questions sur cette collecte de renseignements personnels peuvent être adressées au directeur de (service), (numéro de téléphone), (adresse de l'hôtel de ville), (adresse électronique).

Commissaire à l'information et à la protection de la vie privée de l'Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
CANADA
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site web : www.ipc.on.ca