Lignes directrices sur la vidéosurveillance

Introduction

La surveillance des lieux publics a rapidement augmenté au cours des dernières années. Cette croissance est en grande partie attribuable aux progrès considérables de la technologie de surveillance et à ses prix de plus en plus abordables, ainsi qu'à la perception que la vidéosurveillance renforce la sécurité et la protection du public.

Même si on s'interroge sur l'effet dissuasif de la vidéosurveillance sur la criminalité, il n'en reste pas moins que c'est la raison la plus fréquente pour laquelle les organismes publics et les dépositaires (organisations)* envisagent de recourir à des systèmes de surveillance. Quelle que soit la raison évoquée, il est important de reconnaître que les caméras captent bien d'autres choses que des actes criminels – elles captent aussi des citoyens responsables qui vaquent à leurs occupations quotidiennes. Même si la collecte de ces renseignements peut paraître inoffensive, il existe des lois sur les droits et responsabilités que les organisations doivent respecter en matière de vie privée.

La surveillance omniprésente d'activités légales ordinaires peut grandement entraver le droit à la vie privée d'un individu. Par conséquent, les organisations qui envisagent la mise en place d'un système de surveillance doivent parvenir à un équilibre entre les avantages de la surveillance et le droit à la vie privée des individus dans une société démocratique.

Objet et portée

L'emploi de dispositifs de surveillance étant de plus en plus fréquent au Manitoba, notre bureau estime qu'il est nécessaire d'orienter les organisations qui envisagent d'y recourir. La mise en place d'un système de surveillance exige qu'on l'envisage de façon réfléchie pour réduire au minimum les incidences sur le droit à la vie privée.

Au Manitoba, la Loi sur l'accès à l'information et la protection de la vie privée (LAIPVP) et la Loi sur les renseignements médicaux personnels (LRMP) reconnaissent et protègent le droit d'un particulier à la vie privée. Ces deux lois régissent la collecte, l'utilisation et la communication des renseignements personnels et des renseignements médicaux personnels que détiennent les organisations.

Les présentes lignes directrices visent à aider les organisations à déterminer si un système de surveillance existant ou proposé permet de protéger la vie privée des particuliers.

Aux fins des présentes lignes directrices, nous ne traitons que les activités de surveillance menées par les organismes publics et les dépositaires dans des lieux publics, dans des bâtiments publics et dans les transports publics. Ces lignes directrices ne s'appliquent pas à la surveillance secrète utilisée comme outil d'investigation dans des cas bien précis à des fins d'application de la loi.

Les organisations du secteur privé du Manitoba sont régies par la Loi (fédérale) sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Cette loi énonce les règles de base sur la façon dont les organisations du secteur privé, notamment les entreprises, doivent recueillir, utiliser ou communiquer des renseignements personnels dans le cadre de leurs activités commerciales.

Même si nos lignes directrices portent sur la surveillance dans le secteur public, de nombreuses pratiques exemplaires correspondent aux lignes directrices sur la surveillance dans le secteur privé qui ont été élaborées par le Commissariat à la protection de la vie privée du Canada, et elles peuvent être utiles aux entreprises manitobaines qui envisagent de mettre en place un système de surveillance. Pour obtenir des renseignements précis sur la vidéosurveillance visible et secrète dans le secteur privé, veuillez consulter le site Web du Commissariat :

Surveillance secrète dans le secteur privé : https://www.priv.gc.ca/information/pub/gd_cvs_20090527_f.asp

Surveillance au moyen d'appareils non dissimulés dans le secteur privé : https://www.priv.gc.ca/information/guide/2008/gl_vs_080306_f.asp

Vous envisagez de recourir à la surveillance? Dix principaux éléments à prendre en considération selon l'ombudsman du Manitoba

1 Justification de la surveillance et évaluation de mesures portant moins atteinte à la vie privée

L'utilisation d'un système de surveillance doit être justifiée par des motifs évidents de sécurité ou sur la base d'autres circonstances pouvant être démontrées (par exemple, des signalements précis d'actes criminels).

Les organisations doivent déterminer s'il existe d'autres mesures raisonnables et portant moins atteinte à la vie privée pour protéger la sécurité du public ou détecter ou empêcher les activités criminelles. Elles devraient toujours considérer la vidéo et l'audiosurveillance en dernier recours.

Si les organisations envisagent d'exercer une surveillance, elles devraient évaluer les incidences possibles de la surveillance sur la vie privée des gens. Elles devraient aussi déterminer si la LAIPVP et la LRMP autorisent une telle surveillance.

2 Collecte de renseignements personnels et de renseignements médicaux personnels

Dans le cadre de la LAIPVP et de la LRMP, tout enregistrement de renseignements personnels ou de renseignements médicaux personnels constitue une collecte de renseignements. Avant d'envisager de recourir à un système de surveillance, les organisations doivent déterminer si elles ont le pouvoir de recueillir les renseignements en vertu de certaines dispositions législatives.

De plus, les dispositions législatives en question doivent autoriser chacun des éléments du système de surveillance. Par exemple, si une organisation envisage de mettre en place un système de surveillance qui recueille des séquences audio et vidéo, elle doit être en mesure de prouver la raison et l'autorisation légale de la collecte de ces deux types de séquences. Cela doit inclure des preuves indiquant la façon dont chaque élément respecte l'objet de la collecte. Si l'organisation ne peut pas trouver les dispositions législatives qui autorisent la collecte, elle devrait cesser d'envisager de recourir au système de surveillance.

Pour obtenir d'autres renseignements précis sur la collecte de renseignements personnels et de renseignements médicaux personnels, veuillez consulter les avis de pratique de l'ombudsman du Manitoba intitulés Collecte et avis de collecte de renseignements personnels en vertu de la LAIPVP et Collecte et avis de collecte de renseignements médicaux personnels en vertu de la LRMP dans le site Web du bureau à www.ombudsman.mb.ca.

3 Établissement d'une politique sur les systèmes de surveillance

Si une organisation décide de mettre en place un système de surveillance, elle doit élaborer une politique écrite qui énonce clairement ce qui suit :

- les raisons et les objectifs de l'adoption du système de surveillance
- les dispositions législatives de la LAIPVP ou de la LRMP qui autorisent la collecte de renseignements personnels ou de renseignements médicaux personnels
- l'utilisation qui est faite du matériel de surveillance, notamment :
    - l'endroit où se trouve le matériel,
    - le personnel autorisé à s'en servir

  - le personnel autorisé à se servir du dispositif de stockage ou à y avoir accès
  - les heures de surveillance
- l'information qui sera communiquée au public au sujet du système de surveillance, notamment les renseignements personnels enregistrés, la collecte, l'utilisation, la communication, la conservation, la destruction, la sécurité et l'accès des renseignements personnels et des renseignements médicaux personnels
- la désignation d'un membre du personnel de niveau supérieur chargé des obligations de l'organisation en matière de protection de la vie privée, conformément aux lois et à sa politique, y compris le nom, le titre et le numéro de téléphone
- des directives indiquant les personnes qui sont autorisées à voir les enregistrements, les données audio ou vidéo et dans quelles circonstances, par exemple, en cas d'incident signalé ou soupçonné
- l'obligation pour l'organisation d'avoir en tout temps le contrôle et la responsabilité du système de surveillance
- l'obligation selon laquelle toute entente entre l'organisation et un entrepreneur énonce que les documents créés pendant l'exécution du programme de surveillance sont sous le contrôle de l'organisation et assujettis aux dispositions de la LAIPVP ou de la LRMP, ou des deux, selon le cas
- l'obligation pour les employés et les entrepreneurs d'examiner et de respecter la politique et les dispositions législatives lorsqu'ils accomplissent leurs devoirs et assument leurs fonctions relativement à l'exploitation du système de surveillance, et de signer des ententes écrites au sujet de leurs responsabilités dans le cadre de la politique et de la législation, notamment en se soumettant à un engagement de confidentialité (comme le prévoit la LRMP)
- l'obligation d'avoir en place un processus pour répondre convenablement à toute atteinte à la vie privée (consultez les avis de pratique intitulés Étapes clés de la réponse aux violations du respect de la vie privée en vertu de la LAIPVP et de la LRMP et Rapport d'une violation du respect de la vie privée à l'Ombudsman du Manitoba dans le site Web du bureau à www.ombudsman.mb.ca)
- l'intégration de la politique, y compris les obligations du personnel et des entrepreneurs, dans les programmes réguliers de formation et d'orientation
- un examen ou une mise à jour de la politique tous les deux ans ou plus souvent, si des améliorations ou des changements sont apportés au système de surveillance

4 Conception et mise en oeuvre d'un système de surveillance

Dans la conception d'un système de surveillance, il faut tenir compte de ce qui suit :

- Un système de surveillance ne devrait être installé que dans des lieux publics où la surveillance est un moyen nécessaire et viable de détecter ou d'empêcher des activités criminelles ou de protéger la sécurité du public.
- Le matériel doit être installé de façon à ne surveiller que les espaces considérés comme devant faire l'objet d'une surveillance.
- Si les opérateurs peuvent orienter les caméras, cela devrait être limité, dans la mesure du possible, de façon qu'ils ne puissent pas effectuer de plan rapproché, orienter ou manipuler la caméra pour surveiller des espaces qui ne sont pas prévus au programme de surveillance.
- Le matériel ne doit pas permettre de surveiller l'intérieur d'endroits où les particuliers s'attendent généralement à plus de vie privée, par exemple, l'intérieur de vestiaires et de toilettes.
- Les activités de surveillance doivent se limiter aux périodes pendant lesquelles des activités criminelles risquent manifestement de se produire davantage ou d'être détectées dans la zone surveillée.
- L'accès au système de surveillance doit avoir lieu dans un endroit qui est rigoureusement contrôlé. Seules les personnes qui sont autorisées à se servir du système doivent avoir accès à la zone contrôlée et au matériel de surveillance. Les écrans vidéo ne doivent jamais être installés de façon que le public puisse voir les enregistrements.

5 Avis au public

Il faut aviser le public de façon raisonnable et appropriée que l'on procède à une surveillance ou qu'on est susceptible de le faire.

Une organisation doit être aussi ouverte que possible à propos de son programme de surveillance et elle doit être prête à informer le public au sujet des motifs de la surveillance. Cela consiste notamment à indiquer la raison de la surveillance, l'autorité légale qui autorise la surveillance et les coordonnées de l'employé de l'organisation qui peut répondre aux questions sur la surveillance. Il est possible d'aviser le public de façon raisonnable et appropriée en posant un panneau ou une affiche bien en vue sur le pourtour des zones surveillées.

6 Utilisation et communication des documents de surveillance

Les renseignements recueillis par surveillance audio ou vidéo ne doivent pas être utilisés ni communiqués pour d'autres fins que la fin initiale prévue sauf si des dispositions législatives l'autorisent. Les spécialistes de la protection de la vie privée appellent la pratique consistant à recueillir des renseignements personnels pour une raison particulière et ensuite à utiliser ces renseignements pour une raison différente le « détournement d'usage ». Le détournement d'usage est problématique parce qu'il peut pousser des organisations à utiliser des renseignements personnels en ne respectant pas les exigences de la LAIPVP ou de la LRMP. Par exemple, si une organisation se sert de la vidéosurveillance à l'entrée d'un bâtiment à des fins d'application de la loi et qu'elle souhaite par la suite utiliser les renseignements ainsi recueillis pour contrôler l'assiduité des employés, elle doit tout d'abord déterminer si la loi applicable autorise le nouvel usage des renseignements recueillis, sinon, celui-ci risque d'être illégal.

Les organisations doivent également restreindre l'utilisation des renseignements personnels et des renseignements médicaux personnels aux employés qui ont besoin de les connaître de manière à parvenir à la fin initiale de la collecte. De même, toute communication de renseignements personnels doit être limitée au nombre minimal nécessaire à la réalisation de la fin visée.

Il faut tenir des registres indiquant à quel moment les documents de surveillance ont été utilisés, par qui et à quelle fin. De plus, il faut tenir des registres de tous les cas de communication de documents de surveillance en indiquant les renseignements précis qui ont été communiqués, à qui, à quelle date et pour quelle raison.

7 Conservation et destruction des documents de surveillance

Une organisation doit préparer un calendrier de conservation et de destruction pour préciser pendant combien de temps les documents de surveillance vont être conservés, quand ils vont être détruits et de quelle façon. Le calendrier doit être basé sur une période pendant laquelle un incident réel ou soupçonné risque d'être dévoilé. Si aucun incident réel ou soupçonné n'est dévoilé à la fin de cette période, les renseignements enregistrés au cours de cette période peuvent facilement être effacés ou modifiés. Il faut également établir une période de conservation pour les renseignements qui révèlent des incidents réels; cette période doit permettre de prendre des mesures appropriées en réponse aux données enregistrées, mais elle ne doit pas durer plus longtemps.

Encore une fois, l'organisation doit déterminer la façon dont les documents de surveillance seront détruits à la fin de la période de conservation.

8 Sécurité des documents de surveillance

Tous les dispositifs de stockage doivent être placés en lieu sûr quand on ne s'en sert pas. Par exemple, le stockage en lieu sûr peut inclure la protection par mot de passe d'un appareil numérique rangé dans un contenant verrouillé placé dans une zone dont l'accès est contrôlé. Tous les dispositifs de stockage qui ont été utilisés doivent être datés et numérotés.

Les dispositifs de stockage pouvant être exigés comme éléments de preuve doivent être conservés conformément aux politiques en place jusqu'à ce que les autorités chargées de l'application de la loi les réclament. Avant de transmettre tout dispositif de stockage, il faut remplir un formulaire d'autorisation, qui doit indiquer ce qui suit :

- la personne qui a pris le dispositif
- l'heure et la date auxquelles le dispositif a été pris
- la disposition législative qui a autorisé la remise du dispositif
- la disposition législative qui a autorisé la collecte du dispositif
- si le dispositif sera retourné ou détruit après utilisation.

Il faut régulièrement contrôler toutes les transmissions de dispositifs de stockage et rigoureusement appliquer la politique relative au système de surveillance.

Si la technologie sans fil est utilisée, l'organisation doit crypter de façon sécurisée la transmission sans fil de tous les renseignements personnels ou renseignements médicaux personnels. Il faut faire appel à un spécialiste de la technologie de l'information pour la transmission afin de s'assurer que toutes les mesures technologiques appropriées sont prises.

9 Accès aux documents de surveillance

La loi autorise les particuliers à avoir accès à leurs renseignements personnels et à leurs renseignements médicaux personnels. Cette autorisation s'étend aussi aux documents de surveillance. L'accès peut être accordé pour des renseignements généraux, pour des renseignements personnels ou des renseignements médicaux personnels complets ou partiels, à moins d'une exception prévue par la LAIPVP ou la LRMP.

L'accès aux documents de surveillance dépend aussi de la possibilité, pour les renseignements qui ne peuvent pas être communiqués légalement à un particulier, d'être supprimés d'un enregistrement de façon raisonnable. Par exemple, il est peut-être possible de rendre floues ou de noircir numériquement les images d'autres personnes dans l'enregistrement.

10 Contrôle des systèmes de surveillance

Les organisations doivent périodiquement contrôler l'utilisation et la sécurité du matériel de surveillance, y compris les caméras, les écrans et les dispositifs de stockage, et veiller à ce qu'elles respectent les politiques et procédures opérationnelles. Le contrôle doit aussi porter sur le respect, par les employés, de la LAIPVP ou de la LRMP et de toutes les politiques et procédures connexes. Les résultats de chaque contrôle doivent être consignés et tout manquement ou sujet de préoccupation ressortant de l'exercice doit être réglé.

Les employés et les entrepreneurs qui utilisent le système doivent savoir que leurs activités peuvent faire l'objet d'un contrôle. Une clause de contrôle devrait être ajoutée à tout contrat de services de surveillance. Les organisations devraient régulièrement passer en revue et évaluer leurs systèmes de surveillance pour déterminer si la surveillance est toujours nécessaire ou justifiée.

Conclusion

L'ombudsman du Manitoba veille à l'application de la Loi sur l'accès à l'information et la protection de la vie privée et de la Loi sur les renseignements médicaux personnels en menant des enquêtes et en faisant l'examen des pratiques relatives à l'accès à l'information et à la protection de la vie privée. Il veille au respect des dispositions de la LAIPVP et de la LRMP se rapportant à la protection de la vie privée en procédant à des activités d'enquête, de surveillance et de contrôle. On peut le consulter pour obtenir des conseils sur l'utilisation éventuelle d'un système de surveillance ou sur toute modification ou expansion importante d'un système déjà en place.

Avant qu'elles n'adoptent un système de surveillance, nous recommandons aux organisations d'obtenir des conseils juridiques et de consulter leur coordonnateur ou agent de l'accès à l'information et de la protection de la vie privée. Même si elle n'est pas obligatoire, une évaluation de l'impact sur la vie privée est considérée comme une pratique exemplaire et elle est très utile pour clarifier tout problème éventuel avant la conception et l'installation d'un système de surveillance.

Comme le recours à la vidéo et à l'audiosurveillance entrave grandement le droit à la vie privée et soulève un certain nombre de questions controversées, il faut que les organisations déterminent la véritable nécessité et la valeur de la vidéosurveillance. Il faut qu'elles assurent l'équilibre entre les avantages de la technologie de surveillance et le coût possible sur le plan de la vie privée.

Remerciements

Nous remercions sincèrement le Commissariat à la protection de la vie privée du Canada ainsi que les bureaux des commissaires à l'information et à la protection de la vie privée de la Colombie-Britannique, de l'Alberta, de la Saskatchewan, de l'Ontario, de Terre-Neuve et du Labrador pour leurs contributions à nos Lignes directrices sur la vidéosurveillance. Bon nombre de leurs conseils et connaissances ont été incorporés dans ces lignes directrices.

Ombudsman du Manitoba
Bureau de Winnipeg
500, av. Portage, bur. 750
Winnipeg (Manitoba) R3C 3X1
Tél. : 204-982-9130
Téléc. : 204-942-7803
Sans frais au Manitoba : 1-800-665-0531

ombudsman@ombudsman.mb.ca
www.ombudsman.mb.ca
www.facebook.com/manitobaombudsman

February 2015