TECHNOLOGIE

DÉCEMBRE 2024

Document d'orientation sur l'utilisation de systèmes de reconnaissance des plaques d'immatriculation par les services de police

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

Remerciements

Nous tenons à remercier la Police provinciale de l'Ontario d'avoir passé en revue la version antérieure des présentes lignes directrices, parue en 2017, et de nous avoir fourni de précieux commentaires. La présente version a été établie en consultation avec plusieurs experts, dont des membres d'autres services de police et des universitaires. Nous les remercions également de leurs observations.

TABLE DES MATIÈRES

CONTEXTE

Le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) a publié un premier document d'orientation sur l'utilisation par la police de la technologie de reconnaissance des plaques d'immatriculation (RPI) en 2017. Depuis, en raison de l'évolution de la conjoncture et de nouvelles utilisations de cette technologie, il y a lieu de tenir compte de facteurs et d'enjeux supplémentaires. Nous avons donc mis à jour ce document par souci de clarté et d'uniformité, et pour souligner les aspects essentiels à envisager.

Ces dernières années, l'utilisation de systèmes mobiles de RPI a connu en Ontario un essor considérable, alimenté par des investissements du gouvernement et l'adoption croissante de cette technologie par les services de police. En 2022, le gouvernement de l'Ontario a éliminé les exigences relatives à la vignette d'immatriculation et aux droits de renouvellement connexes pour les véhicules de tourisme, les camions légers, les motocyclettes et les cyclomoteurs[1]. À la place, pour améliorer la sécurité publique et renforcer les contrôles routiers, le gouvernement a accordé aux services policiers une subvention ponctuelle pour les inciter à adopter cette technologie.

Certains services de police de l'Ontario utilisaient déjà des systèmes mobiles de RPI avant 2022, mais cette subvention a permis l'acquisition de nouveaux systèmes plus perfectionnés, dotés de caméras, de logiciels et d'une interopérabilité améliorés. Certains services de police ont été en mesure de doter tous leurs véhicules de cette technologie. La subvention a également permis aux services qui n'utilisaient pas déjà cette technologie d'en faire l'acquisition et de l'implanter. Ainsi, de nombreux systèmes de RPI sont déployés maintenant dans toute la province.

En Ontario, les systèmes de RPI sont généralement installés dans les véhicules de police. Cependant, ils peuvent également être installés dans des endroits fixes, comme des poteaux téléphoniques ou des ponts d'étagement. De plus, il est possible d'intégrer les logiciels de RPI dans d'autres technologies policières, comme les systèmes de caméras de bord (SCB) et de télévision en circuit fermé (TVCF), renforçant ainsi les capacités de ces systèmes et technologies.

Les systèmes fixes de RPI posent d'importants risques supplémentaires en matière de vie privée et de surveillance, et le CIPVP a mis à jour ses lignes directrices en conséquence.

INTRODUCTION

Les systèmes de RPI peuvent être configurés en mode mobile ou fixe. La technologie de RPI peut lire rapidement un grand nombre de numéros de plaques d'immatriculation et les comparer à des listes de plaques contenues dans une base de données. Les systèmes de RPI se composent d'éléments tels une caméra, un ordinateur et une base de données[2]. Les services de police de l'Ontario utilisent les systèmes de RPI pour déterminer si les numéros de plaques d'immatriculation captés en temps réel sur les routes se retrouvent sur des listes de plaques volées ou expirées, appartenant à des conducteurs dont le permis a été suspendu ou associées à des personnes disparues ou à des alertes Amber ayant fait intervenir un véhicule.

1 Communiqué de février 2022 du gouvernement de l'Ontario, **L'Ontario met fin aux droits de renouvellement des plaques d'immatriculation et aux exigences relatives à la vignette d'immatriculation**.

2 Les systèmes de RPI sont également appelés systèmes informatisés de reconnaissance des numéros de plaque d'immatriculation.

Les systèmes de RPI recueillent également d'autres renseignements personnels lorsqu'ils lisent une plaque d'immatriculation, dont la date, l'heure et la géolocalisation du véhicule. Ces systèmes peuvent ainsi être employés pour suivre les déplacements d'une personne, ce qui accroît le risque de surveillance et de profilage.

L'utilisation sans restriction des systèmes de RPI suscite de sérieuses préoccupations en matière de vie privée. Bien qu'il importe d'assurer la sécurité publique, le service de police doit utiliser les systèmes de RPI dans le respect des lois ontariennes sur la protection de la vie privée s'appliquant au secteur public et des attentes raisonnables du public en matière de vie privée et des autres libertés et droits fondamentaux. Il est essentiel d'adopter des politiques, des procédures et des contrôles techniques appropriés afin de protéger la vie privée, d'autant plus que la plupart des conducteurs dont les véhicules sont contrôlés par les systèmes de RPI se livrent simplement à leurs activités quotidiennes.

Le CIPVP surveille la conformité à la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (LAIMPVP), qui s'applique aux services de police municipaux, et à la *Loi sur l'accès à l'information et la protection de la vie privée* (LAIPVP), qui s'applique à la Police provinciale de l'Ontario[3].

Le présent document énonce les principales obligations des services de police en vertu de la LAIMPVP et de la LAIPVP quant à l'utilisation de systèmes de RPI, et il fournit une orientation, y compris des pratiques exemplaires, sur l'utilisation de ces systèmes dans le respect de la vie privée. Il aborde l'utilisation par la police de systèmes mobiles et fixes de RPI à des fins précises de sécurité publique, notamment pour alerter un policier qui effectue un contrôle routier au sujet d'une plaque d'immatriculation. Il ne traite pas du recours à des systèmes de RPI pour la gestion de la circulation, le péage routier, l'application des règlements de stationnement ou la tenue d'enquêtes, ni de l'intégration de la RPI dans d'autres technologies. Ces autres contextes soulèvent des questions différentes en matière de vie privée, et pourraient nécessiter d'autres démarches pour en atténuer l'incidence. En outre, les systèmes policiers de RPI pourraient être assujettis à des obligations et restrictions légales dont il faut tenir compte en plus de celles qui sont établies dans la LAIMPVP et la LAIPVP.

DÉFINITIONS

- **Correspondance** – Fait pour une plaque d'immatriculation lue de correspondre à une plaque se trouvant sur une liste noire.
- **Données de correspondance** – Données associées à une correspondance qui sont recueillies par le système de RPI, par exemple, images des plaques, date, heure et informations de géolocalisation.
- **Données de non-correspondance** – Données associées à une non-correspondance qui sont recueillies par le système de RPI, par exemple, images des plaques, date, heure et informations de géolocalisation.
- **Liste noire** – Liste des plaques d'immatriculation que la police ou des institutions affiliées, telles que le ministère des Transports (MTO), ont identifiées comme étant recherchées (il s'agit

3 La Police provinciale de l'Ontario n'est pas une institution en vertu de la LAIPVP, mais elle y est assujettie car elle relève du ministère de la Sécurité communautaire et des Services correctionnels. Pour ce qui est des services de police municipaux, les commissions municipales des services policiers sont les institutions visées par la LAIMPVP, mais les services de police sont assujettis eux aussi à la LAIMPVP.

d'un type de liste de surveillance). Les services de police reçoivent généralement des listes noires actualisées quotidiennement du MTO et du Centre d'information de la police canadienne (CIPC), qu'ils peuvent étoffer manuellement dans certaines situations précises. Les listes noires sont stockées dans la base de données du système de RPI et transmises à un ordinateur situé dans le véhicule de police. Voir les annexes A et B pour des précisions sur les listes noires.

- **Non-correspondance** – Fait pour une plaque d'immatriculation lue de ne pas correspondre à une plaque se trouvant sur une liste noire; ce terme s'applique aussi aux correspondances inexactes.
- **Reconnaissance des plaques d'immatriculation (RPI)** – Technologie comprenant une caméra, un ordinateur et une base de données, qui forment ensemble un « système de RPI ». Installé dans un véhicule ou sur un objet stationnaire, le système de RPI est employé pour identifier des véhicules en déterminant si le numéro de leur plaque d'immatriculation se trouve sur des listes stockées dans une base de données.
- **Service de police** – S'entend d'un service de police municipal, d'une commission municipale des services policiers et de la Police provinciale de l'Ontario[4].

QU'EST-CE QUE LA TECHNOLOGIE DE RPI?

En général, un système de RPI fonctionne de la façon suivante :

1. Une caméra capte automatiquement toutes les plaques d'immatriculation qui sont à sa portée. Deux images sont captées : une image de la plaque elle-même, et une image contextuelle permettant de déterminer la marque, le modèle et la couleur du véhicule. Les images contextuelles peuvent montrer par inadvertance des personnes comme les occupants du véhicule ou des piétons. Le système, selon ses paramètres, peut aussi consigner la date, l'heure et des informations de géolocalisation associées à l'image de la plaque.
2. L'ordinateur utilise un logiciel pour analyser les images afin d'extraire et de numériser les données sur les plaques pour traitement.
3. Lorsqu'une plaque lue semble correspondre à une plaque se trouvant sur une liste noire, le système alerte le service de police. Un policier tente ensuite de confirmer visuellement qu'il s'agit bien d'une correspondance possible en comparant l'image de la plaque aux données numérisées sur les plaques contenues dans le système de RPI. Une correspondance peut entraîner l'affichage de données supplémentaires sur le véhicule, comme la marque, le modèle, l'année et la couleur, ce qui permet au policier de confirmer et d'agir.
4. Lorsque cette correspondance révèle que le propriétaire enregistré de la plaque en question est un conducteur dont le permis a été suspendu, le système donne son nom et d'autres renseignements, comme le fait qu'il doit porter ou non des lunettes ou des lentilles cornéennes. Le policier peut utiliser d'autres systèmes pour identifier clairement le conducteur et le véhicule si ce dernier fait l'objet d'un contrôle.
5. Lorsque la correspondance a été confirmée manuellement, un policier peut prendre les mesures qui s'imposent, comme demander au conducteur de se ranger pour effectuer un

4 Dans le présent document, toute mention des commissions des services policiers s'entend également du solliciteur général, dont relève la Police provinciale de l'Ontario.

contrôle, lui donner une contravention pour avoir conduit avec une immatriculation expirée, ou vérifier si le propriétaire du véhicule dont le permis est suspendu est bien la personne qui est au volant.

6. Les non-correspondances ne sont pas signalées aux policiers, qui n'ont donc rien à faire quand elles se produisent.

Les systèmes de RPI peuvent également capter et extraire des renseignements inexacts. Par exemple, une plaque recouverte de boue pourrait être mal interprétée par le système. Il peut arriver aussi que le numéro de plaque soit bien lu et extrait, mais que la province d'origine soit erronée. Pour ces raisons, le policier doit confirmer que les correspondances sont valables et qu'il peut y donner suite, qu'il utilise un système de RPI mobile ou fixe.

Selon la configuration du système, les données de correspondance peuvent être consignées dans l'ordinateur qui se trouve dans le véhicule de police ou dans un serveur de la police situé à distance.

TYPES DE TECHNOLOGIES DE RPI

Les **systèmes mobiles de RPI** sont installés dans des véhicules de police. Les caméras peuvent être fixées à l'extérieur du véhicule pour capter des images de plaques d'immatriculation devant et derrière le véhicule. Au lieu de telles caméras extérieures, il est également possible d'intégrer un logiciel de RPI dans les systèmes de caméras de bord (SCB); ces caméras sont installées à l'intérieur du véhicule de police. Une caméra est dirigée vers l'extérieur, pour capter des images hors du véhicule, et une autre est orientée vers l'intérieur, pour capter des images de ce qui se passe dans le véhicule. Les systèmes mobiles de RPI peuvent lire continuellement les plaques d'immatriculation pendant leur fonctionnement, par exemple, lors de patrouilles.

Les **systèmes fixes de RPI** comprennent des caméras fixes installées à des endroits stratégiques : ponts d'étagement, lampadaires, poteaux téléphoniques ou de signalisation, etc. Ces systèmes fixes peuvent fonctionner 24 heures sur 24, tous les jours, et lire continuellement toutes les plaques d'immatriculation qui sont à portée de la caméra, même lorsque les véhicules se déplacent à haute vitesse. Si des caméras de RPI multiples sont installées le long d'une voie publique, les données recueillies peuvent révéler les déplacements d'un véhicule entre deux emplacements à des moments précis.

RENSEIGNEMENTS PERSONNELS

Le service de police doit se conformer aux règles sur la protection de la vie privée établies dans la LAIMPVP et la LAIPVP lorsqu'il recueille, conserve, utilise ou divulgue des « renseignements personnels ». Le paragraphe 2 (1) de la LAIMPVP et de la LAIPVP définit « renseignements personnels » comme des « renseignements consignés ayant trait à un particulier qui peut être identifié », ce qui s'entend notamment « d'un numéro d'identification, d'un symbole ou d'un autre signe individuel qui lui est attribué ».

Le CIPVP a déjà statué que le numéro de plaque d'immatriculation d'un véhicule appartenant à un particulier est un renseignement personnel[5]. Un particulier reçoit une plaque d'immatriculation à

5 Ordonnances **M-336** et **MO-1863** et enquête sur la protection de la vie privée **MC-030023-1** du CIPVP.

l'achat d'un véhicule et la conserve quand il le revend. Comme la plaque est associée au particulier, elle peut révéler des renseignements à son sujet. Par conséquent, les règles énoncées dans la LAIMPVP et la LAIPVP concernant les renseignements personnels s'appliquent généralement aux services de police qui recueillent ou utilisent des numéros de plaques d'immatriculation. L'emplacement, l'heure et la date associés à une plaque d'immatriculation sont aussi des renseignements personnels. Le système de RPI d'un service de police et les politiques, procédures et contrôles techniques qui y sont associés doivent donc se conformer également aux lois ontariennes sur la protection de la vie privée qui régissent le secteur public.

INCIDENCE DES SYSTÈMES DE RPI SUR LA VIE PRIVÉE

La RPI peut se révéler utile pour l'exécution de la loi, mais elle peut aussi poser des risques importants pour la vie privée des particuliers. En plus de se conformer à la LAIMPVP et à la LAIPVP, le service de police doit faire en sorte que son système de RPI respecte le droit à la vie privée reconnu en vertu de la *Charte canadienne des droits et libertés*. La Cour suprême du Canada a reconnu un droit à la vie privée dans les lieux publics, y compris sur la voie publique[6]. L'adoption de politiques, de procédures et de contrôles techniques adéquats peut permettre de s'assurer que les renseignements personnels sont traités de façon conforme à la loi.

La technologie de RPI n'est pas nouvelle, mais le nombre de systèmes de RPI que la police utilise pour surveiller les routes ontariennes a connu une croissance importante ces dernières années, et cette tendance se maintiendra probablement. L'expansion de ces systèmes dans la province et leur capacité accrue à recueillir plus de données en exacerbent les risques liés à la protection de la vie privée et à la surveillance, comme nous en discuterons dans les sections suivantes.

Comme ces systèmes se multiplient, de plus en plus de plaques d'immatriculation sont lues tous les jours, de même que des données contextuelles, de sorte que la quantité de données de RPI que la police doit recueillir, gérer et protéger augmente à un rythme exponentiel. Les erreurs système ou humaines donnant lieu à des erreurs de lecture ou d'identification pourraient également devenir plus fréquentes et présenter des conséquences indésirables et sérieuses pour les particuliers concernés. Par exemple, la plaque d'un véhicule appartenant à un conducteur dont le permis a été suspendu se retrouvera sur une liste noire. Si elle est détectée, le système de RPI alertera le policier, qui pourrait demander au conducteur de se ranger pour un contrôle routier. Or, le conducteur n'est pas nécessairement le propriétaire enregistré du véhicule. Ainsi, certaines personnes pourraient être interceptées à plusieurs reprises, et une telle situation se répercuterait sur les deuxièmes conducteurs ou les familles dont les membres se partagent un véhicule ou le prêtent à d'autres familles.

La multiplication des systèmes de RPI dans la province a donné lieu à la création d'un réseau de surveillance étendu qui est mieux en mesure de retracer les déplacements de véhicules et de conducteurs en associant plusieurs correspondances obtenues au moyen de caméras multiples. Ainsi, il pourrait être plus facile pour la police de faire le suivi des déplacements d'un conducteur et de son véhicule, compte tenu surtout du fait que ces systèmes consignent la date, l'heure et l'emplacement approximatif des véhicules dont la plaque est lue. Si ces données sont conservées par la police, elles pourraient avec le temps révéler des habitudes de déplacement à l'intérieur d'une même ville ou dans la province, permettant de faire des déductions au sujet de particuliers, par exemple, les endroits où ils se rendent souvent ou leurs destinations inhabituelles.

6 *R c. Spencer*, 2014 CSC 43, par. 44; *R c. Wise*, [1992] 1 RCS 527, p. 564-565.

Les particuliers qui se sentent observés peuvent modifier certaines activités ou éviter de s'y adonner, et être dissuadés de participer à des activités légales comme obtenir des soins médicaux, prendre part à des manifestations pacifiques ou réclamer des changements sociaux. Les systèmes de RPI peuvent causer des problèmes imprévus, tels qu'un effet néfaste sur la liberté d'expression et d'association.

La police devrait donc faire preuve de transparence et mener des consultations sur le recours à la RPI, adopter des politiques et procédures détaillées ainsi que concevoir et configurer ses systèmes avec soin afin de protéger le droit à la vie privée et les autres droits fondamentaux du public.

CONFIGURATION DU SYSTÈME

La plupart des systèmes de RPI peuvent présenter diverses configurations. Le service de police devrait configurer son système pour ses risques pour la vie privée, en respectant ses politiques et procédures. Par exemple, il doit s'assurer que les caméras du système captent uniquement la plaque d'immatriculation et non les occupants du véhicule ou les piétons. Il est recommandé d'adopter une approche de **protection intégrée de la vie privée** afin d'enchâsser la protection de la vie privée dans le système dès sa conception et sa configuration.

Si les caméras du système captent par inadvertance autre chose que la plaque d'immatriculation, tout renseignement personnel devrait être caviardé conformément aux politiques et procédures pertinentes du service de police, par exemple, en brouillant les images pour dissimuler l'identité des particuliers photographiés. Afin que seuls les renseignements personnels requis soient recueillis, il pourrait également être nécessaire de modifier le nombre de caméras ou leur emplacement.

Le système devrait également être configuré de façon à éviter que les contrôles ne soient manipulés ou contournés. Les utilisateurs d'un système de RPI ne devraient pas pouvoir modifier ou reconfigurer l'appareil ou le système sans autorisation. Le système devrait consigner dans un journal tout changement à sa configuration.

Le service de police peut collaborer avec des fournisseurs de technologie pour se procurer un système de RPI, le configurer et le mettre en œuvre, mais il lui incombe toujours de respecter les lois ontariennes sur la protection de la vie privée. Chaque service de police devrait consulter le document d'orientation ***La protection de la vie privée et l'accès à l'information dans les contrats du secteur public avec des fournisseurs externes*** du CIPVP, qui contient des recommandations en matière de protection de la vie privée et de transparence dans le contexte du recours à des fournisseurs de services externes.

ÉVALUATION DE L'IMPACT SUR LA VIE PRIVÉE (EIVP)

Le service de police qui souhaite implanter un système de RPI, même s'il s'agit d'un projet pilote, ou apporter des modifications importantes à un système existant devrait déterminer au préalable son incidence éventuelle sur la vie privée en menant une évaluation de l'impact sur la vie privée (EIVP). Cette évaluation définit les impacts réels et éventuels d'un programme ou d'une activité sur la vie privée d'un particulier ainsi que les précautions à prendre et les stratégies à adopter pour éliminer ces effets négatifs ou les ramener à un niveau acceptable. Le service de police devrait mettre à jour son EIVP avant d'apporter des changements importants à son programme de RPI.

L'EIVP devrait relever et aborder les aspects relatifs à l'utilisation d'un système de RPI, notamment :

- les règles encadrant l'utilisation du système;
- l'objet et la portée du programme, y compris les critères régissant les listes noires;
- les règles concernant la collecte, la conservation, l'utilisation, la divulgation et l'élimination des renseignements personnels et la portée de ces activités;
- la question de savoir si un système de RPI est nécessaire et se révélera efficace pour un service de police en déterminant clairement ses objectifs et ses utilisations prévues;
- la question de savoir s'il serait possible d'obtenir des résultats semblables au moyen de méthodes qui portent moins atteinte à la vie privée;
- une justification du nombre et de l'emplacement des caméras, surtout de caméras fixes à des endroits précis;
- les règles concernant les avis publics et l'accès des particuliers aux renseignements;
- les caractéristiques et les aspects techniques nécessaires pour assurer l'intégrité du système et de son fonctionnement;
- les politiques visant à assurer la reddition de comptes et la surveillance;
- les mesures de sécurité visant à protéger les renseignements personnels;
- les examens et audits périodiques des objectifs et utilisations du programme et de son efficacité globale.

Les services de police peuvent consulter le document ***Planifier pour réussir : Guide d'évaluation de l'incidence sur la vie privée*** du CIPVP pour obtenir des conseils sur la tenue d'une EIVP.

AUTRES FACTEURS CONCERNANT LES SYSTÈMES FIXES DE RPI

Selon leur configuration, les systèmes fixes de RPI peuvent capter continuellement les plaques d'immatriculation de tous les véhicules qui passent à un endroit particulier ou qui arrivent et quittent un secteur précis. Ces systèmes posent donc des risques supplémentaires liés à la protection de la vie privée et à la surveillance dont le service de police doit tenir compte dans son EIVP, ses politiques et ses procédures, ainsi que lors des consultations publiques préalables au déploiement.

La nécessité, la proportionnalité et la transparence des systèmes fixes de RPI revêtent une importance particulière. Pour déterminer s'il est nécessaire d'installer des caméras fixes de RPI, le service de police devrait déterminer soigneusement combien en installer et à quels endroits, dans le but d'aider les policiers à effectuer des contrôles routiers immédiats. Il devrait aussi réévaluer régulièrement l'emplacement des caméras pour déterminer si celles-ci entraînent des conséquences imprévues ou négatives, et établir s'il est toujours nécessaire et proportionnel de disposer d'une caméra à un endroit particulier ou si la caméra devrait être retirée.

La police devrait notamment déterminer l'incidence des caméras fixes de RPI sur certaines communautés si elles sont installées près de secteurs sensibles, par exemple, à des endroits où il y a des manifestations, près de lieux de culte ou aux entrées ou sorties d'une ville. Combiner des

systèmes fixes de RPI à des systèmes mobiles existants ou à d'autres technologies pourrait rendre encore plus complexe le programme de RPI d'un service de police et en accroître les risques pour la vie privée.

L'installation de caméras fixes de RPI devrait être précédée de consultations publiques et de la divulgation de tous les emplacements prévus pour ces caméras. Des recommandations quant aux avis, à la transparence et à la participation du public figurent dans la section du présent document portant sur les politiques et procédures.

CONSULTATION DU CIPVP

Le service de police devrait consulter le CIPVP dans les circonstances suivantes, pour s'assurer de bien tenir compte des questions touchant la protection de la vie privée:

- modification ou élargissement important de son programme de RPI[7], surtout s'il envisage de nouvelles configurations, des systèmes fixes de RPI ou la combinaison de la technologie de RPI avec d'autres technologies, comme les caméras de télévision en circuit fermé ou l'analytique vidéo;
- élargissement possible d'une liste noire à des catégories autres que celles énumérées aux annexes A et B;
- utilisation possible des données de RPI à des fins de maintien de l'ordre autres que les contrôles routiers immédiats.

MENER UN PROJET PILOTE

Le service de police qui envisage de déployer un système mobile ou fixe de RPI ou d'apporter des changements importants à un système existant devrait procéder à un projet pilote de durée limitée avant la mise en place définitive. Un projet pilote permet de déterminer la fonctionnalité, la sécurité, la transparence et la nécessité du système, et d'établir s'il assure la protection de la vie privée. L'évaluation des résultats du projet pilote aidera la police à apporter les modifications nécessaires aux éléments clés de son programme, y compris l'EIVP et les politiques et procédures.

Le service de police devrait planifier son projet pilote en suivant les étapes suivantes :

- définir l'objet, les buts, les objectifs et la portée du projet pilote;
- déterminer ce qui sera mesuré au cours du projet pilote (p. ex., des indicateurs liés à la configuration du système, à la fonctionnalité des appareils, à l'efficacité des contrôles de confidentialité et de sécurité) et en faire part au public;
- déterminer le soutien administratif requis aux fins de la collecte et de l'analyse des données, afin de guider le projet pilote et son évaluation;

7 En 2003, le CIPVP a fait enquête sur l'utilisation par le Service de police de Toronto d'un système de RPI pour retracer des véhicules volés (voir l'enquête sur la protection de la vie privée **MC-030023-1**). Le CIPVP a alors déclaré que les institutions, y compris les organismes de maintien de l'ordre, devraient le consulter avant de lancer des initiatives semblables qui peuvent avoir une incidence sur la vie privée.

- consulter et renseigner le public sur le projet pilote et les prochaines étapes, en particulier les personnes susceptibles d'être touchées par le programme de RPI, et demander l'avis des organisations concernées, y compris des groupes de la société civile;
- justifier clairement le nombre et l'emplacement des caméras requises, et particulièrement l'installation de caméras fixes à certains emplacements ou dans certaines collectivités;
- évaluer et documenter toute différence opérationnelle entre les systèmes de RPI mobiles et fixes quant aux suites données aux correspondances;
- déterminer si les avantages escomptés du système de RPI ont été obtenus et si des risques ou préjudices imprévus sont apparus.

POLITIQUES ET PROCÉDURES

Il est essentiel d'élaborer et d'appliquer des politiques et procédures exhaustives sur l'utilisation des systèmes de RPI. Ces politiques et procédures devraient notamment donner une orientation sur l'utilisation appropriée du système de RPI par les policiers et d'autres utilisateurs, et prévoir des examens et audits réguliers. La section suivante décrit les aspects sur lesquels les politiques et procédures de RPI devraient porter.

PORTÉE ET OBJET DU PROGRAMME ET RÈGLES QUI L'ENCADRENT

Le service de police doit s'assurer que la LAIMPVP ou la LAIPVP l'autorise à recueillir, à conserver, à utiliser et à divulguer les renseignements personnels que permet d'obtenir un système de RPI. Au moment de concevoir et de mettre en œuvre son programme, il doit veiller à ce que ce dernier fonctionne conformément à la portée de ses obligations et pouvoirs relatifs aux contrôles routiers. Les politiques et procédures devraient mentionner à quelles fins il est justifié d'utiliser un système de RPI, ainsi que les fins auxquelles les renseignements personnels seront utilisés.

COLLECTE

Le système de RPI lit toutes les plaques d'immatriculation qui sont à la portée de sa caméra. Ainsi, un véhicule muni d'un tel système ou une caméra fixe de RPI recueillera des renseignements sur les activités quotidiennes de milliers de personnes. Un grand nombre de ces lectures ne donneront pas lieu à des correspondances et ne seront donc pas pertinentes compte tenu de l'objet du programme.

Le paragraphe 28 (2) de la LAIMPVP et le paragraphe 38 (2) de la LAIPVP interdisent la collecte de renseignements personnels pour le compte d'une institution, sauf si :

1. elle est autorisée expressément par une loi;
2. ces renseignements servent à l'exécution de la loi;
3. ces renseignements sont nécessaires au bon exercice d'une activité autorisée par la loi.

L'institution doit répondre à au moins un de ces trois critères pour être autorisée à recueillir des renseignements personnels. Dans la plupart des cas, le service de police s'attardera au deuxième

critère (**les renseignements servent à l'exécution de la loi**) pour établir la portée, l'objet, la conception et les modalités de fonctionnement d'un programme de RPI.

Pour être visée par la définition d'« exécution de la loi » du paragraphe 2 (1) de LAIMPVP et de la LAIPVP, la collecte doit être effectuée soit pour le « maintien de l'ordre », soit pour « des enquêtes ou inspections qui aboutissent ou peuvent aboutir à des instances devant les tribunaux judiciaires ou administratifs, si ceux-ci peuvent imposer une peine ou une sanction à l'issue de ces instances ».

Le CIPVP a statué que l'expression « servent à l'exécution de la loi » ne confère pas un pouvoir inconditionnel et ne s'applique que dans les cas où la collecte de renseignements personnels **facilite effectivement l'exécution de la loi**[8]. En ce qui concerne la RPI, les renseignements personnels recueillis par la police pourraient être utilisés pour alerter un policier en patrouille de la présence d'une plaque d'immatriculation dans des circonstances où il serait généralement justifié de demander d'effectuer un contrôle routier en demandant au conducteur de s'immobiliser. Cela pourrait se produire dans les situations où le policier confirme que la plaque ou le véhicule a été volé, que le permis de conduire du propriétaire enregistré de la plaque a été suspendu ou encore que ce propriétaire n'est pas assuré, fait l'objet d'un mandat d'arrêt ou est associé à une alerte Amber.

Pour l'administration d'un programme de RPI, la police pourrait recueillir des renseignements personnels auprès d'un tiers, comme le MTO, le CIPC ou un autre service de police. Les renseignements personnels recueillis auprès du MTO et du CIPC comprennent une liste noire de plaques d'immatriculation qui est actualisée quotidiennement. Chaque service de police peut également communiquer des plaques d'immatriculation d'intérêt à d'autres services à des fins de correspondance.

Pour assurer le respect de la LAIMPVP et de la LAIPVP, le service de police devrait envisager de conclure des ententes d'échange de renseignements avec des tiers. Ces ententes devraient définir l'autorité légale permettant l'échange de renseignements et les droits et obligations de toutes les parties concernant le traitement de renseignements personnels. Si de telles ententes n'ont pas déjà été conclues, le service de police devrait consulter ses conseillers juridiques et son personnel chargé de la protection de la vie privée.

AVIS

La LAIMPVP et la LAIPVP obligent les institutions à informer les particuliers de la collecte de renseignements personnels les concernant, sous réserve de certaines exceptions[9]. Ainsi, selon le paragraphe 29 (2) de la LAIMPVP et le paragraphe 39 (2) de la LAIPVP, l'institution doit informer le particulier :

a. de l'autorité légale invoquée pour la collecte;

b. des fins principales auxquelles doivent servir ces renseignements personnels;

c. du titre, de l'adresse et du numéro de téléphone d'affaires d'un fonctionnaire public qui peut renseigner le particulier au sujet de cette collecte.

8 CIPVP, rapport sur une plainte concernant la protection de la vie privée **MC-040012-1**.

9 Le paragraphe 29 (3) de la LAIMPVP et le paragraphe 39 (3) de la LAIPVP prévoient des exceptions aux règles sur les avis pour certaines fins liées à l'exécution de la loi. Soulignons que l'application de ces exceptions est établie au cas par cas.

Le service de police devrait rédiger et donner des avis appropriés et suffisamment transparents pour informer le public du fait qu'il utilisera la RPI avant son implantation.

Avis visuel : Dans le cas des systèmes mobiles de RPI, un avis devrait être inscrit, dans la mesure du possible, sur les véhicules de police munis d'un tel système pour informer le public de son utilisation.

Dans le cas des systèmes fixes de RPI, des affiches devraient être installées à des endroits visibles au périmètre des zones surveillées. Ces affiches devraient indiquer clairement qu'un système fixe de RPI est en cours d'utilisation, et inclure les renseignements requis en vertu des alinéas 29 (2) a) à c) de la LAIMPVP et du paragraphe 39 (2) de la LAIPVP, comme indiqué plus haut.

Avis verbal : Sauf dans des circonstances où on craint pour la sécurité du public ou du policier, un policier qui effectue un contrôle routier à la suite d'une correspondance devrait informer le particulier en question de l'utilisation d'un système de RPI.

TRANSPARENCE

Le service de police devrait informer le public de l'utilisation de systèmes de RPI dans les médias locaux, par des campagnes dans les médias sociaux et dans son site Web. Il doit également s'assurer que les renseignements requis en vertu des alinéas 29 (2) a) à c) de la LAIMPVP et des alinéas 39 (2) a) à c) de la LAIPVP sont disponibles et faciles d'accès dans son site Web.

Dans le cas des systèmes fixes de RPI, le service de police devrait consulter le public et lui donner un avis écrit avant l'installation et la mise en service de ces systèmes.

En outre, le service de police devrait publier dans son site Web des renseignements à jour sur son programme ou projet pilote de RPI, notamment :

- la version la plus récente des politiques de RPI et des procédures connexes du service de police;
- une description des renseignements recueillis au moyen de la RPI et des fins auxquelles ils sont recueillis;
- une description du programme de RPI du service de police, y compris le nombre et les types de véhicules munis de caméras mobiles et l'emplacement des caméras fixes;
- les périodes de conservation applicables;
- la procédure que les particuliers doivent suivre pour porter plainte sur l'utilisation ou l'emplacement des caméras de RPI ou sur le fait qu'une plaque a été inscrite sur une liste noire (voir la section **Mécanismes de présentation de plaintes et de recours**);
- la façon dont les particuliers peuvent demander à visionner les images et les données connexes du système de RPI ou à y avoir accès, ou demander qu'elles soient rendues publiques;
- la marche à suivre pour interjeter appel au CIPVP lorsque la demande d'accès à l'information est refusée en tout ou en partie;

- la procédure que les particuliers doivent suivre pour demander l'accès à leurs renseignements personnels et leur rectification (p. ex., la rectification d'inscriptions sur la liste noire qui sont fondées sur des renseignements erronés ou périmés);
- une copie du dernier rapport annuel du service de police à sa commission.

UTILISATION

L'article 31 de la LAIMPVP et le paragraphe 41 (1) de la LAIPVP limitent l'utilisation des renseignements personnels qui sont recueillis conformément à ces lois. Celles-ci interdisent à l'institution d'utiliser des renseignements personnels sauf :

- si la personne concernée par ces renseignements a consenti à leur utilisation;
- aux fins pour lesquelles ils ont été obtenus ou recueillis ou à des fins compatibles;
- à des fins qui justifient leur divulgation à l'institution en vertu de l'article 32 de la LAIMPVP ou du paragraphe 42 (1) de la LAIPVP.

Une « fin compatible » est définie à l'article 33 de la LAIMPVP et à l'article 43 de la LAIPVP comme étant la fin invoquée à l'appui de l'utilisation de renseignements personnels à laquelle le particulier concerné par les renseignements pourrait raisonnablement s'attendre lorsque ceux-ci ont été obtenus du particulier directement. L'utilisation de renseignements personnels à d'autres fins n'est pas permise, sous réserve des exceptions susmentionnées.

Les renseignements personnels recueillis par un système de RPI d'un service de police se divisent généralement en trois catégories : les renseignements inscrits sur des listes noires, les données de correspondance et, pendant une très brève période, les données de non-correspondance. Le service de police devrait déterminer comment et par qui sont utilisées les listes noires et les données de correspondance, pour s'assurer qu'elles sont employées uniquement à des fins autorisées. Le système devrait supprimer les données de non-correspondance aussitôt après leur collecte, tel que décrit dans la section suivante. La description de la façon dont est gérée chacune de ces catégories de renseignements contribuera à assurer la transparence et la reddition de comptes quant à leur utilisation de façon appropriée dans le respect de la vie privée.

CHAMP D'APPLICATION DES LISTES NOIRES

Le fait qu'un numéro de plaque d'immatriculation figure sur une liste noire peut se répercuter de façon importante sur le droit à la vie privée d'un particulier et sur son droit de se déplacer librement au sein de la collectivité. C'est pourquoi les politiques et procédures de RPI doivent assortir le champ d'application et la conception des listes noires de limites strictes et prévoir une surveillance appropriée.

Le contenu d'une liste noire et les catégories de plaques qui y figurent doivent être soigneusement encadrés par des normes précises et objectives qui sont reliées aux fins légales de la liste. Les catégories de plaques qu'il est permis de recueillir auprès du MTO et du CIPC sont énumérées à l'annexe A. Les catégories permises pour les inscriptions manuelles figurent à l'annexe B[10]. Les listes noires devraient contenir uniquement les catégories de plaques énumérées aux annexes A et B.

10 Le CIPVP a établi les annexes A et B à la suite de consultations avec la Police provinciale de l'Ontario.

Une liste noire qui va au-delà des catégories énumérées aux annexes A et B pourrait avoir une incidence déraisonnable sur la vie privée des personnes concernées. Si un service de police juge nécessaire d'inclure des plaques qui ne font pas partie de ces catégories, il devrait consulter le CIPVP au préalable.

Les politiques et procédures du service de police concernant la RPI devraient préciser les listes noires employées, les catégories de plaques autorisées sur chaque liste noire ainsi que l'organisme responsable de dresser chaque liste.

INSCRIPTIONS MANUELLES

En plus de recevoir des listes noires d'institutions comme le MTO, les policiers peuvent ajouter manuellement des plaques d'immatriculation à une liste noire. Il est important que les politiques et les procédures définissent les circonstances précises et limitées dans lesquelles il est possible d'ajouter manuellement des plaques ou de les communiquer à d'autres services de police. Par exemple, une saisie manuelle pourrait être permise dans le cas d'une plaque associée à une alerte Amber ou à une personne portée disparue. Les circonstances dans lesquelles une modification manuelle à une liste noire est permise devraient être détaillées et exhaustives, et aucun autre type d'inscription manuelle ne devrait être autorisé. Comme indiqué plus haut, la police devrait limiter les inscriptions manuelles aux catégories énumérées à l'annexe B.

Les politiques et procédures concernant la RPI devraient aussi préciser les renseignements que le policier doit inclure lorsqu'il inscrit manuellement une plaque d'immatriculation dans le système, comme son nom et son numéro d'identification unique (p. ex., son matricule), la raison pour laquelle il inscrit cette plaque ainsi que la période pendant laquelle celle-ci demeurera sur la liste noire. Les politiques devraient prévoir une période appropriée.

Les plaques devraient figurer sur une liste noire uniquement pendant la période où cela est raisonnablement nécessaire, après quoi elles doivent être retirées de tous les systèmes de RPI. La politique devrait également préciser si les renseignements sur la plaque doivent s'accompagner, dans le champ des commentaires, d'une description physique du conducteur enregistré ou associé à la plaque.

En outre, la politique devrait préciser si une telle inscription manuelle devrait être communiquée aux listes noires de tous les autres utilisateurs de systèmes de RPI de l'Ontario, ou se trouver uniquement sur la liste noire interne du service de police en question. Cependant, une plaque inscrite manuellement dont on croit qu'elle est utilisée par un conducteur dont le permis est suspendu mais qui n'est pas enregistrée à son nom doit figurer uniquement sur la liste noire interne du service de police, et ne pas être communiquée à tous les autres utilisateurs de systèmes de RPI de l'Ontario (voir l'annexe B).

RECHERCHES MANUELLES

Le système de RPI lit automatiquement les plaques d'immatriculation, mais il pourrait permettre aussi au policier de vérifier manuellement si une plaque d'immatriculation se trouve sur une liste noire ou si elle a été incluse dans les correspondances ou non-correspondances captées par le système. Comme dans le cas des autres bases de données policières, comme celle du CIPC, il pourrait être

approprié pour un policier d'effectuer une telle vérification manuellement. Les politiques concernant la RPI devraient décrire les circonstances où les policiers sont autorisés à effectuer une recherche de plaque manuelle et celles où ils n'y sont pas autorisés. Par exemple, les politiques devraient interdire aux policiers d'utiliser la fonction de recherche manuelle pour des motifs autres qu'une enquête criminelle en cours.

Le service de police devrait configurer le système de RPI de façon à consigner dans un journal toutes les recherches manuelles. Ce journal devrait contenir l'identité du policier qui a effectué la recherche, la date et l'heure, une description de la recherche manuelle et de ses motifs et tout numéro de dossier connexe.

GESTION DES DONNÉES DE CORRESPONDANCE ET DES DONNÉES DE NON-CORRESPONDANCE

Les systèmes de RPI sont utilisés pour déterminer si une plaque se trouve sur une liste noire. Lorsqu'un policier confirme visuellement qu'une correspondance est bel et bien exacte, les données sur cette correspondance peuvent être conservées et utilisées à des fins connexes d'exécution de la loi et lors d'instances judiciaires. Par exemple, si une plaque d'immatriculation volée a été localisée, les données sur cette correspondance peuvent être utilisées pour faire enquête sur le vol et intenter des poursuites.

Les données de non-correspondance devraient être recueillies ou utilisées brièvement, et uniquement pour déterminer si une plaque d'immatriculation qui a été lue donne lieu ou non à une correspondance. Lorsqu'il est établi qu'il y a non-correspondance, la LAIMPVP ou la LAIPVP n'autorise plus sa collecte, sa conservation ou son utilisation.

Les données de non-correspondance devraient être supprimées dès qu'il est possible de le faire sur le plan technologique, et il ne faut pas y accéder ni les utiliser avant leur suppression, sauf si la loi autorise expressément cet accès ou cette utilisation. Avant d'accéder à des données de non-correspondance et de les utiliser, le service de police devrait consulter ses avocats pour déterminer s'il dispose de l'autorité légale requise pour le faire (p. ex., en vertu d'une ordonnance de communication). Entre-temps, le service peut conserver un ensemble limité de données de non-correspondance jusqu'à ce que la question de l'autorité légale soit réglée (p. ex., des données de non-correspondance associées à un emplacement ou à un secteur précis, à une période donnée et à une enquête criminelle connexe précise), mais il doit supprimer immédiatement toutes les autres données de non-correspondance. Une fois réglée la question de l'autorité légale, toutes les données de non-correspondance que le service de police avait conservées mais auxquelles il n'est pas autorisé à avoir accès ou à utiliser doivent également être supprimées immédiatement.

UTILISATIONS SECONDAIRES DES DONNÉES DE CORRESPONDANCE RECUEILLIES AU MOYEN DE LA RPI

Le service de police devrait utiliser les renseignements sur les correspondances recueillis au moyen du programme de RPI uniquement aux fins précises et définies de ce programme visant l'exécution de la loi, par exemple, alerter un policier en patrouille de la présence d'une plaque d'immatriculation dont le numéro se trouve sur une liste noire dans les situations où il serait justifié d'arrêter un véhicule pour un contrôle routier et de mener une enquête et d'autres activités d'exécution de la loi.

Le service de police ne devrait pas utiliser de données de RPI, y compris des données de correspondance, à des fins secondaires, comme le suivi en temps réel ou historique de l'emplacement et des déplacements d'un particulier, à moins que la loi ne l'y autorise expressément.

ACCÈS INTERNE AU SYSTÈME DE RPI

Au sein d'un service de police, l'accès à un système de RPI devrait être réservé à un nombre limité de personnes autorisées. Ces personnes devraient faire l'objet de contrôles d'accès basés sur les rôles, qui sont documentés et accordés selon le principe d'accès sélectif. Il est important de consigner dans un journal tous les accès au système de RPI et toutes les utilisations de ce système. Les fichiers journaux devraient identifier l'utilisateur du système par son nom et son numéro d'identification unique (comme son matricule), et indiquer l'heure d'accès, les renseignements consultés ainsi que le motif de l'accès au système et de son utilisation.

DIVULGATION

La LAIMPVP et la LAIPVP interdisent la divulgation de renseignements personnels, sauf dans les situations énoncées à l'article 32 de la LAIMPVP et au paragraphe 42 (1) de la LAIPVP. Comme dans le cas de l'utilisation de renseignements personnels, les lois permettent à un service de police de divulguer des renseignements personnels aux fins pour lesquelles ils ont été obtenus ou recueillis ou à des fins compatibles. Les politiques et procédures de RPI devraient préciser les cas où les renseignements personnels recueillis au moyen du système peuvent être divulgués.

Le service de police devrait aussi tenir un journal contenant des renseignements sur chaque divulgation, c'est-à-dire :

- l'autorité légale invoquée pour la divulgation, y compris une description des circonstances justifiant la divulgation et des renvois aux ententes de partage de renseignements en vigueur;
- l'identité du policier qui a autorisé la divulgation;
- la date, l'heure et le lieu de la collecte;
- tout document associé à la plaque;
- le nom et le titre du tiers à qui les renseignements sont divulgués et, s'il y a lieu, le numéro de dossier de la partie qui fait la divulgation ou de l'enquête du tiers;
- une description des renseignements en cause, notamment les numéros de plaque divulgués, leur type ou la catégorie de la liste noire dont ils font partie;
- les moyens employés pour divulguer les renseignements;
- une description des conditions qui limitent le droit du tiers d'utiliser et de divulguer les renseignements;
- le fait de savoir si le destinataire renverra ou détruira de façon sécurisée les renseignements après utilisation.

CONSERVATION

La LAIMPVP, la LAIPVP et leurs règlements d'application prévoient des règles sur la période de conservation des renseignements personnels que les institutions utilisent. Plus précisément, aux termes de l'article 5 du Règlement 823 pris en application de la LAIMPVP et du paragraphe 5 (1) du Règlement 460 pris en application de la LAIPVP, les institutions doivent conserver ces renseignements pendant au moins un an après leur utilisation à moins que le particulier ne consente à leur suppression avant la fin de ce délai. Le Règlement 823 pris en application de la LAIMPVP permet aux institutions municipales de réduire ce délai par résolution ou règlement. Lorsqu'on établit que des renseignements recueillis par la RPI sont liés à une correspondance qui a été confirmée, le service de police doit les conserver conformément à ces règles. Évidemment, comme les données de correspondance peuvent être reliées à une enquête ou à une instance particulière, il pourrait y avoir des exigences relatives à la conservation qui s'ajoutent à celles qui sont énoncées dans ces règlements.

Par contre, le service de police doit supprimer immédiatement toutes les données de non-correspondance dès qu'il est possible de le faire sur le plan technologique, qu'elles se trouvent dans l'ordinateur du véhicule ou dans un serveur de la police (voir la section **Gestion des données de correspondance et des données de non-correspondance**).

Le service de police devrait modifier ses pratiques relatives aux renseignements, règlements, résolutions, etc., afin de se conformer à ces exigences.

EXACTITUDE

Le service de police devrait actualiser toutes les listes noires sauvegardées dans ses serveurs centraux et les ordinateurs de ses véhicules de police au besoin pour s'assurer qu'elles sont exactes et à jour[11]. La plupart des systèmes de RPI peuvent être configurés pour une mise à jour quotidienne. Lorsqu'une inscription est supprimée d'une liste noire, elle devrait aussi être supprimée de toutes les autres listes noires de RPI dès que possible. En outre, les politiques, procédures et systèmes de RPI devraient faciliter l'élimination régulière des inscriptions en double, expirées ou erronées des listes noires. Les mises à jour des bases de données devraient être consignées dans un journal à des fins de reddition de comptes.

SÉCURITÉ

L'article 3 du Règlement 823 pris en application de la LAIMPVP et l'article 4 du Règlement 460 pris en application de la LAIPVP obligent les institutions à déterminer, documenter et appliquer des mesures raisonnables pour empêcher l'accès non autorisé aux documents et éviter que ces documents ne soient détruits ou endommagés par inadvertance. Le service de police doit donc adopter des politiques et procédures pour assurer le traitement sécurisé des renseignements personnels.

Le service de police devrait prendre les mesures de sécurité suivantes :

- ***Transfert sécurisé*** : Veiller à sécuriser les renseignements transférés vers des serveurs, et de ceux-ci aux véhicules de police.

11 Soulignons que le paragraphe 30 (3) de la LAIMPVP et le paragraphe 40 (3) de la LAIPVP prévoient des exceptions aux dispositions de la loi sur l'exactitude aux fins de l'exécution de la loi.

- ***Stockage sécurisé*** : Chiffrer tous les renseignements liés à la RPI quand ils ne sont pas utilisés, sans égard au lieu de stockage.
- ***Sécurité matérielle*** : Conserver de façon sécurisée le matériel et les documents de RPI, comme les disques, cartes mémoire ou serveurs, afin d'éviter le vol, la perte ou l'accès non autorisé. Tenir compte de l'emplacement des caméras fixes de RPI et prendre des mesures de sécurité pour éviter qu'elles ne soient sabotées, endommagées, perdues ou volées ou qu'on n'y accède sans autorisation.
- ***Contrôles d'accès*** : Permettre uniquement aux personnes qui ont besoin des renseignements recueillis par RPI pour leurs fonctions d'y avoir accès.
- ***Effacement sécurisé*** : Détruire de façon permanente les renseignements périmés, inexacts ou superflus.
- ***Minimisation des données*** : Concevoir, configurer et utiliser le système de RPI afin que seuls les renseignements personnels nécessaires soient recueillis, conservés, utilisés et divulgués.
- ***Configuration*** : Normaliser les configurations visant à sécuriser le système de RPI dans l'ensemble du service, et ne pas utiliser les réglages implicites ou de base.
- ***Maintenance*** : Installer régulièrement les correctifs élaborés pour le système et ses applications afin d'éviter toute vulnérabilité.
- ***Journalisation*** : Tenir un journal de tous les accès aux renseignements recueillis par RPI et des utilisations et divulgations de ces renseignements à des fins d'audit. Ce journal devrait être généré automatiquement lorsque les documents sont conservés sous forme électronique.
- ***Surveillance des activités*** : Surveiller le fonctionnement du système de RPI et intervenir lorsqu'on soupçonne une atteinte à la vie privée ou à la sécurité, un incident ou une anomalie.
- ***Évaluation des risques*** : Évaluer régulièrement les risques et mener d'autres examens opérationnels afin d'évaluer les mesures de sécurité d'en améliorer l'efficacité.

Le service de police devrait instaurer des protocoles en vue de déceler et de maîtriser les atteintes à la sécurité et à la vie privée, de faire enquête à leur sujet et de prendre des mesures visant à en atténuer les conséquences. Le document ***Les atteintes à la vie privée : Lignes directrices pour les organismes du secteur public*** contient des lignes directrices sur l'élaboration de procédures de gestion des atteintes à la vie privée.

EXAMENS ET AUDITS

La surveillance opérationnelle est essentielle pour assurer la reddition de comptes et protéger la vie privée dans le contexte de l'utilisation d'un système de RPI. Des audits et examens réguliers s'imposent pour évaluer et améliorer le programme de RPI.

Le service de police devrait surveiller couramment les journaux d'accès au système pour déceler les anomalies et les infractions aux politiques et procédures, et effectuer notamment des vérifications aléatoires d'utilisateurs particuliers. Les policiers devraient être informés du fait que leurs activités

pourraient faire l'objet d'un audit et d'une surveillance, et qu'ils pourraient être appelés à justifier leur utilisation du système.

Le service de police devrait examiner régulièrement la technologie, les contrôles et le rendement opérationnel du système de RPI pour s'assurer que ce dernier:

- demeure efficace;
- est conforme aux politiques et procédures;
- est toujours nécessaire et proportionnel.

En outre, ces politiques et procédures devraient être examinées régulièrement et mises à jour chaque fois qu'un changement important est apporté au système de RPI. Ces examens devraient être confiés à un tiers indépendant, et il faudrait combler toute lacune ou donner suite à toute préoccupation dans les plus brefs délais.

Le service de police devrait aussi envisager de publier un rapport annuel sur l'utilisation de son système de RPI décrivant les objectifs du programme, les activités de déploiement et les principales statistiques opérationnelles. Un tel rapport permet de faire preuve de transparence au sujet de l'utilisation du système; rendre compte de son efficacité pourrait accroître l'appui que lui accorde le public.

FORMATION

Le fonctionnement efficace d'un système de RPI et la conformité à la LAIMPVP et à la LAIPVP sont tributaires du respect des politiques et procédures. Le service de police doit donc fournir une formation appropriée à tous ceux qui ont accès au système.

La formation initiale et continue devrait comprendre des directives claires sur les rôles, obligations et autres responsabilités. Les utilisateurs (policiers, autres employés, fournisseurs de services de l'extérieur) devraient recevoir un exemplaire des politiques et procédures, et signer une entente attestant qu'ils se conformeront aux pratiques établies et respecteront la confidentialité. La formation devrait comprendre aussi un exposé des mesures disciplinaires auxquelles s'exposent ceux qui enfreignent les politiques et procédures du service de police.

Toutes les politiques et procédures applicables devraient être mises à la disposition des policiers, administrateurs de la TI et autres membres du personnel chargés du fonctionnement du programme, ainsi que des fournisseurs de services de l'extérieur.

MÉCANISMES DE PRÉSENTATION DE PLAINTES ET DE RECOURS

Les politiques et procédures de RPI devraient préciser comment les particuliers peuvent porter plainte et demander à être rayés du système lorsqu'ils sont d'avis que leur plaque d'immatriculation ne devrait pas se trouver sur une liste noire. Lorsque l'inscription sur une liste noire concernant un particulier provient d'un autre service de police ou organisme ou d'une autre institution, comme la Gendarmerie royale du Canada, le particulier devrait recevoir le nom et les coordonnées du responsable des inscriptions sur la liste noire et de la réception des plaintes ou demandes de recours afin de pouvoir faire retirer cette inscription.

Le service de police devrait aussi informer le public de son droit de déposer une plainte concernant la protection de la vie privée auprès du CIPVP conformément à la LAIMPVP ou à la LAIPVP, selon le cas.

Le service de police devrait mettre ces renseignements, ainsi que d'autres renseignements sur ses politiques et procédures de RPI, à la disposition du public sur son site Web.

DEMANDES D'ACCÈS À L'INFORMATION

En Ontario, les particuliers ont le droit d'accéder aux documents dont les institutions ont la garde ou le contrôle en vertu de l'article 4 de la LAIMPVP et de l'article 10 de la LAIPVP. De plus, les particuliers à l'égard desquels des institutions ont la garde ou le contrôle de renseignements personnels ont le droit d'accéder à ces renseignements et de demander leur rectification en vertu du paragraphe 36 (1) de la LAIMPVP et du paragraphe 47 (1) de la LAIPVP.

Un service de police peut recevoir une demande d'un particulier qui souhaite savoir, par exemple, si sa plaque d'immatriculation est ou était inscrite sur la liste noire, ou obtenir l'accès à des documents associés à la collecte, à l'utilisation ou à la divulgation de sa plaque. Ce service doit donc établir un processus afin de pouvoir répondre aux demandes d'accès dans le délai prévu par la loi.

Soulignons que les particuliers ont le droit de demander l'accès à de tels documents, mais qu'une partie ou la totalité d'entre eux pourrait être exemptée de divulgation en vertu de la LAIMPVP et de la LAIPVP. Par exemple, l'article 38 de la LAIMPVP et l'article 49 de la LAIPVP prévoient des exceptions, notamment lorsque la divulgation représenterait une atteinte injustifiée à la vie privée d'un autre particulier. Le service de police devrait consulter son coordonnateur de l'accès à l'information et de la protection de la vie privée pour obtenir des conseils sur la façon de répondre aux demandes d'accès à l'information.

Le service de police qui refuse une demande d'accès à l'information doit informer l'auteur de la demande de son droit d'interjeter appel au CIPVP.

CONCLUSION

Les systèmes de RPI aident les services de police à relever rapidement les plaques d'immatriculation se trouvant sur des listes noires à des fins d'enquête et d'exécution de la loi. La police utilise de plus en plus la RPI, ce qui donne lieu à des conséquences importantes en matière de protection de la vie privée et de surveillance. Les systèmes de RPI permettent de recueillir, de conserver et d'utiliser des renseignements personnels concernant des particuliers qui se livrent à leurs activités quotidiennes. Les systèmes fixes de RPI, en particulier, peuvent capter continuellement les plaques d'immatriculation de tous les véhicules qui passent à un endroit précis ou qui sont à leur portée. L'atteinte à la vie privée qui en résulte peut avoir des répercussions considérables sur les droits et libertés fondamentaux. C'est pourquoi il faut mettre en place des politiques, procédures et contrôles techniques appropriés afin d'assurer la confidentialité, la sécurité, la fonctionnalité et la nécessité du programme de RPI, qu'il soit mobile ou fixe.

Si le programme de RPI est implanté de façon légale, transparente et respectueuse de la vie privée, comme il est décrit dans les présentes lignes directrices, les risques qu'il pose pour le droit à la vie privée et d'autres droits s'en trouveront atténués, et les services de police pourront atteindre leurs objectifs en matière de sécurité publique tout en respectant leurs obligations en vertu de la LAIMPVP et de la LAIPVP.

ANNEXE A : CATÉGORIES DE PLAQUES CONSIGNÉES PAR LE MINISTÈRE DES TRANSPORTS (MTO) ET LE CENTRE D'INFORMATION DE LA POLICE CANADIENNE (CIPC)

Renseignements fournis par le MTO

- Plaques portant une vignette d'immatriculation expirée
- Plaques annulées
- Plaques manquantes, perdues ou volées
- Plaques suspendues (en la possession du titulaire ou du MTO)
- Plaques non délivrées et plaques volées non délivrées
- Plaques abîmées
- Plaques non fixées
- Plaques associées à des conducteurs dont le permis a été suspendu
- Plaques associées à des conducteurs qui ne sont pas titulaires de permis

Renseignements fournis par le CIPC

- Plaques volées
- Plaques associées à des véhicules volés (voitures, camions, motos)
- Plaques associées à des personnes qui sont visées par un mandat

ANNEXE B : CATÉGORIES DE PLAQUES POUR L'INSCRIPTION MANUELLE

- Plaques enregistrées au nom de personnes qui font l'objet d'une enquête criminelle en cours
- Plaques correspondant à un véhicule dont on sait qu'il a été impliqué directement dans une activité criminelle faisant l'objet d'une enquête criminelle en cours
- Plaques enregistrées au nom de personnes dont le permis de conduire a été suspendu pendant une courte période pour une infraction liée à la consommation d'alcool ou au *Code de la route* et dont on croit qu'elles pourraient continuer de conduire leur véhicule pendant la période de suspension
- Plaques associées à des personnes disparues
- Plaques associées à une alerte Amber
- Plaques non enregistrées mais dont on a raison de croire qu'elles sont utilisées par des conducteurs dont le permis de conduire a été suspendu et dont le dossier en vertu du *Code de la route* suscite des inquiétudes en matière de sécurité publique. Les données sur les plaques faisant l'objet d'une inscription manuelle doivent :
    - être ajoutées uniquement à la liste noire interne du service, et **ne pas** être distribuées à tous les autres utilisateurs de systèmes de RPI;
    - demeurer sur la liste noire interne du service pendant un maximum de 30 jours, après quoi elles doivent être supprimées;
    - être accompagnées dans le champ « commentaires » d'une description physique du conducteur suspendu afin de distinguer ce dernier des autres conducteurs, y compris le propriétaire enregistré de la plaque.

ANNEXE C : RÉSUMÉ DES PRINCIPALES RECOMMANDATIONS

Voici un sommaire des principales recommandations à des fins d'information uniquement. Veuillez consulter la section correspondante du présent document d'orientation pour obtenir des précisions et des exigences précises.

Le CIPVP formule les recommandations suivantes aux services de police pour la mise en œuvre d'un programme de reconnaissance des plaques d'immatriculation (RPI) en Ontario :

CONFIGURATION DU SYSTÈME

- Configurer le système de RPI de façon à atténuer les risques pour la vie privée et conformément aux politiques et procédures du service de police. Par exemple, il faut s'assurer que les caméras du système captent uniquement la plaque d'immatriculation et non les occupants du véhicule ou les piétons.
- Adopter une approche de protection intégrée de la vie privée en enchâssant la protection de la vie privée dès la conception et la configuration du système.
- Si les caméras du système captent par inadvertance autre chose que la plaque d'immatriculation, tout renseignement personnel devrait être caviardé conformément aux politiques et procédures applicables.
- Afin que seuls les renseignements personnels requis soient recueillis, il pourrait également être nécessaire de modifier le nombre de caméras ou leur emplacement.
- Le système devrait également être configuré de façon à éviter que les contrôles ne soient manipulés ou contournés.
- Les utilisateurs d'un système de RPI ne devraient pas pouvoir modifier ou reconfigurer l'appareil ou le système sans autorisation.
- Le système devrait consigner dans un journal tout changement à sa configuration.

EFFECTUER UNE ÉVALUATION DE L'IMPACT SUR LA VIE PRIVÉE (EIVP)

- Le service de police qui souhaite implanter un système de RPI, même s'il s'agit d'un projet pilote, ou apporter des modifications importantes à un système existant devrait déterminer au préalable son incidence éventuelle sur la vie privée en menant une EIVP.
- Le service de police devrait mettre à jour son EIVP avant d'apporter des changements importants à son programme de RPI.
- L'EIVP devrait relever et régler les aspects touchant la protection de la vie privée en lien avec l'utilisation de technologies de RPI, y compris les autres facteurs concernant les systèmes fixes de RPI qui sont abordés dans le présent document.

CONSULTATION DU CIPVP

- Nous invitons les services de police à consulter le CIPVP afin de tenir compte de façon appropriée des questions touchant la protection de la vie privée dans les circonstances suivantes :
    - modification ou élargissement important de leur programme de RPI, surtout s'ils envisagent de nouvelles configurations, des systèmes fixes de RPI ou la combinaison de la technologie de RPI à d'autres technologies comme les caméras de télévision en circuit fermé ou l'analytique vidéo;
    - élargissement possible d'une liste noire à des catégories autres que celles énumérées aux annexes A et B;
    - utilisation possible des données de RPI à des fins de maintien de l'ordre autres que les contrôles routiers immédiats.

MENER UN PROJET PILOTE

- Le service de police qui envisage de déployer un système mobile ou fixe de RPI ou d'apporter des changements importants à un système existant devrait procéder à un projet pilote de durée limitée avant la mise en place définitive.
- L'évaluation des résultats du projet pilote aidera la police à apporter les modifications nécessaires aux éléments clés de son programme, y compris l'EIVP et les politiques et procédures.
- Le service de police devrait planifier son projet pilote en suivant les étapes énoncées dans le présent document.

POLITIQUES ET PROCÉDURES

- Il est essentiel d'élaborer et d'appliquer des politiques et procédures exhaustives sur l'utilisation des systèmes de RPI.
- Les politiques et procédures de RPI devraient notamment donner une orientation sur l'utilisation appropriée du système de RPI par les policiers et d'autres utilisateurs, et prévoir des examens et audits réguliers.

PORTÉE ET OBJET DU PROGRAMME ET RÈGLES QUI L'ENCADRENT

- Le service de police doit s'assurer que la LAIMPVP ou la LAIPVP l'autorise à recueillir, à conserver, à utiliser et à divulguer les renseignements personnels que permet d'obtenir un système de RPI.
- Au moment de concevoir et de mettre en œuvre leur programme, il doit veiller à ce que ce dernier fonctionne conformément à la portée de ses obligations et pouvoirs relatifs aux contrôles routiers.

- • Les politiques et procédures devraient mentionner à quelles fins il est justifié d'utiliser un système de RPI, y compris les fins auxquelles les renseignements personnels seront utilisés.

COLLECTE

- L'institution doit répondre à au moins un des trois critères énoncés au paragraphe 28 (2) de la LAIMPVP et au paragraphe 38 (2) de la LAIPVP pour être autorisée à recueillir des renseignements personnels.
- Pour assurer la conformité à la LAIMPVP et à la LAIPVP, le service de police devrait envisager de conclure des ententes d'échange de renseignements avec des tiers.
- Ces ententes devraient définir l'autorité légale permettant l'échange de renseignements et les droits et obligations de toutes les parties concernant le traitement de renseignements personnels.
- Si de telles ententes n'ont pas déjà été conclues, le service de police devrait consulter ses conseillers juridiques et son personnel chargé de la protection de la vie privée.

AVIS

- Les institutions doivent informer les particuliers de la collecte de renseignements personnels les concernant, sous réserve de certaines exceptions.
- Le service de police devrait élaborer et donner des avis visuels et verbaux appropriés et suffisamment transparents pour informer le public du fait qu'il utilisera la RPI avant son implantation.
- **Avis visuel** :
    - Dans le cas des systèmes mobiles de RPI, un avis devrait être inscrit, dans la mesure du possible, sur les véhicules de police munis d'un tel système pour informer le public de son utilisation.
    - Dans le cas des systèmes fixes de RPI, des affiches devraient être installées à des endroits visibles au périmètre des zones surveillées. Ces affiches devraient indiquer clairement qu'un système fixe de RPI est en cours d'utilisation, et inclure les renseignements requis en vertu des alinéas 29 (2) a) à c) de la LAIMPVP et du paragraphe 39 (2) de la LAIPVP, comme indiqué dans le présent document.
- **Avis verbal** :
    - Sauf dans des circonstances où on craint pour la sécurité du public ou du policier, un policier qui effectue un contrôle routier à la suite d'une correspondance devrait informer le particulier en question de l'utilisation d'un système de RPI.

TRANSPARENCE

- Le service de police devrait informer le public de l'utilisation de systèmes de RPI dans les médias locaux, par des campagnes dans les médias sociaux et dans son site Web.
- Il doit également s'assurer que les renseignements indiqués aux alinéas 29 (2) a) à c) de la LAIMPVP et aux alinéas 39 (2) a) à c) de la LAIPVP sont disponibles et faciles d'accès dans son site Web.
- Dans le cas des systèmes fixes de RPI, le service de police devrait consulter le public et lui donner un avis écrit avant l'installation et la mise en service de ces systèmes.
- Le service de police devrait publier dans son site Web des renseignements à jour sur son programme ou projet pilote de RPI, y compris ce qui est indiqué dans le présent document.

UTILISATION

- Les renseignements personnels recueillis par un système de RPI d'un service de police se divisent généralement en trois catégories : les renseignements inscrits sur des listes noires, les données de correspondance et, pendant une très brève période, les données de non-correspondance. Le service de police devrait déterminer comment et par qui sont utilisées les listes noires et les données de correspondance, pour s'assurer qu'elles sont employées uniquement à des fins autorisées.
- Le système devrait supprimer les données de non-correspondance aussitôt après leur collecte.
- La description de la façon dont est gérée chacune de ces catégories de renseignements contribuera à assurer la transparence et la reddition de comptes quant à leur utilisation de façon appropriée dans le respect de la vie privée.

CHAMP D'APPLICATION DES LISTES NOIRES

- Les politiques et procédures de RPI du service de police doivent assortir le champ d'application et la conception des listes noires de limites strictes et prévoir une surveillance appropriée.
- Le contenu d'une liste noire et les catégories de plaques qui y figurent doivent être soigneusement encadrés par des normes précises et objectives qui sont reliées aux fins légales de la liste.
- Pour ses listes noires, le service de police devrait s'en tenir uniquement aux catégories figurant dans ces deux annexes.
- Si un service de police juge nécessaire d'inclure des plaques qui ne font pas partie de ces catégories, il devrait consulter le CIPVP au préalable.
- Les politiques et procédures d'un service de police concernant la RPI devraient prévoir les listes noires employées, les catégories de plaques autorisées sur chaque liste noire ainsi que l'organisme responsable de dresser chaque liste.

INSCRIPTIONS MANUELLES

- Il est important que les politiques et les procédures définissent les circonstances précises et limitées dans lesquelles il est possible d'ajouter manuellement des plaques ou de les communiquer à d'autres services de police.
- Les circonstances dans lesquelles une modification manuelle à une liste noire est permise devraient être détaillées et exhaustives, et aucun autre type d'inscription manuelle ne devrait être autorisé.
- Le service de police devrait limiter les inscriptions manuelles aux catégories énumérées à l'annexe B.
- Les politiques et procédures concernant la RPI devraient aussi préciser les renseignements que le policier doit inclure lorsqu'il saisit manuellement une plaque d'immatriculation dans le système.
- Les plaques devraient figurer sur une liste noire uniquement pendant la période où cela est raisonnablement nécessaire, après quoi elles doivent être retirées de tous les systèmes de RPI.
- Le service de police devrait déterminer si une inscription manuelle devrait être communiquée aux listes noires de tous les autres utilisateurs de systèmes de RPI de l'Ontario ou se trouver uniquement sur sa liste noire interne.
- Une plaque inscrite manuellement dont on croit qu'elle est utilisée par un conducteur dont le permis est suspendu mais qui n'est pas enregistrée à son nom **doit** figurer uniquement sur la liste noire du service de police en question, et ne doit pas être communiquée à tous les autres utilisateurs de systèmes de RPI de l'Ontario (voir l'annexe B).

RECHERCHES MANUELLES

- Les politiques concernant la RPI devraient décrire les circonstances où les policiers sont autorisés à effectuer une recherche de plaque manuelle et celles où ils n'y sont pas autorisés.
- Les politiques devraient interdire aux policiers d'utiliser la fonction de recherche manuelle pour des motifs autres qu'une enquête criminelle en cours.
- Le service de police devrait configurer le système de RPI de façon à consigner dans un journal toutes les recherches manuelles. Ce journal devrait contenir l'identité du policier qui a effectué la recherche, la date et l'heure, une description de la recherche manuelle et de ses motifs et tout numéro de dossier connexe.

GESTION DES DONNÉES DE CORRESPONDANCE ET DES DONNÉES DE NON-CORRESPONDANCE

- Lorsqu'un policier confirme visuellement qu'une correspondance est bel et bien exacte, les données sur cette correspondance peuvent être conservées et utilisées à des fins connexes d'exécution de la loi et lors d'instances judiciaires.

- Les données de non-correspondance devraient être recueillies ou utilisées brièvement, et uniquement pour déterminer si une plaque d'immatriculation qui a été lue donne lieu ou non à une correspondance.
- Les données de non-correspondance devraient être supprimées dès qu'il est possible de le faire sur le plan technologique, et il ne faut pas y accéder ni les utiliser avant leur suppression, sauf si la loi autorise manifestement cet accès ou cette utilisation.
- Avant d'accéder à des données de non-correspondance et de les utiliser, le service de police devrait consulter ses avocats pour déterminer s'il dispose de l'autorité légale requise pour le faire.
- Entre-temps, le service peut conserver un ensemble limité de données de non-correspondance jusqu'à ce que la question de l'autorité légale soit réglée, mais il doit supprimer immédiatement toutes les autres données de non-correspondance.
- Dès que la question de l'autorité légale est réglée, toutes les données de non-correspondance que le service de police avait conservées mais auxquelles il n'est pas autorisé à avoir accès ou qu'il ne peut pas utiliser doivent également être supprimées immédiatement.

UTILISATIONS SECONDAIRES DES DONNÉES DE RPI

- Le service de police devrait utiliser les renseignements sur les correspondances recueillis au moyen du programme de RPI uniquement aux fins précises et définies de ce programme visant l'exécution de la loi, par exemple, alerter un policier en patrouille de la présence d'une plaque d'immatriculation dont le numéro se trouve sur une liste noire dans les situations où il serait justifié d'arrêter un véhicule pour un contrôle routier et de mener une enquête et d'autres activités d'exécution de la loi.
- Le service de police ne devrait pas utiliser de données de RPI, y compris des données de correspondance, à des fins secondaires, comme le suivi en temps réel ou historique de l'emplacement et des déplacements d'un particulier, à moins que la loi ne l'y autorise expressément.

ACCÈS INTERNE AU SYSTÈME DE RPI

- Au sein d'un service de police, l'accès à un système de RPI devrait être réservé à un nombre limité de personnes autorisées. Ces personnes devraient faire l'objet de contrôles d'accès basés sur les rôles, qui sont documentés et accordés selon le principe d'accès sélectif.
- Tous les accès au système de RPI et toutes les utilisations de ce système devraient être consignés dans un journal.
- Les fichiers journaux devraient identifier l'utilisateur du système par son nom et son numéro d'identification unique (comme son matricule), et indiquer l'heure d'accès, les renseignements consultés ainsi que le motif de l'accès au système et de son utilisation.

DIVULGATION

- Les politiques et procédures de RPI devraient préciser les cas où les renseignements personnels recueillis au moyen du système peuvent être divulgués.
- Le service de police devrait aussi tenir un journal contenant des renseignements sur chaque divulgation, comprenant les renseignements indiqués dans le présent document.

CONSERVATION

- Lorsqu'on établit que des renseignements recueillis par la RPI sont liés à une correspondance qui a été confirmée, le service de police doit les conserver conformément à la LAIMPVP, à la LAIPVP et à leurs règlements d'application.
- Contrairement aux données de correspondance, le service de police doit supprimer immédiatement toutes les données de non-correspondance dès qu'il est possible de le faire sur le plan technologique, qu'elles se trouvent dans l'ordinateur du véhicule ou dans un serveur de la police.
- Le service de police devrait modifier ses pratiques relatives aux renseignements, règlements, résolutions, etc., afin de se conformer à ces exigences.

EXACTITUDE

- Le service de police devrait actualiser toutes les listes noires sauvegardées dans ses serveurs centraux et les ordinateurs des véhicules de police au besoin pour s'assurer qu'elles sont exactes et à jour.
- Lorsqu'une inscription est supprimée d'une liste noire, elle devrait aussi être supprimée de toutes les listes noires de RPI dès que possible.
- Les politiques, procédures et systèmes de RPI devraient faciliter l'élimination régulière des inscriptions en double, expirées ou erronées des listes noires.
- Les mises à jour des bases de données devraient être consignées dans un journal à des fins de reddition de comptes.

SÉCURITÉ

- Le service de police doit adopter des politiques et procédures pour assurer le traitement sécurisé des renseignements personnels.
- Le service de police devrait prendre les mesures de sécurité décrites dans le présent document : transfert sécurisé, stockage sécurisé, sécurité matérielle, contrôles d'accès, effacement sécurisé, minimisation des données, configuration, maintenance, journalisation, surveillance des activités et évaluation des risques.

- Le service de police devrait instaurer des protocoles en vue de relever et de maîtriser les atteintes à la sécurité et à la vie privée, de faire enquête à leur sujet et de prendre des mesures visant à en atténuer les conséquences.

EXAMENS ET AUDITS

- Des audits et examens réguliers s'imposent pour évaluer et améliorer le programme de RPI.
- Le service de police devrait surveiller couramment les journaux d'accès au système pour déceler les anomalies et les infractions aux politiques et procédures, et effectuer notamment des vérifications aléatoires d'utilisateurs particuliers.
- Le service de police devrait examiner régulièrement la technologie, les contrôles et le rendement opérationnel du système de RPI pour s'assurer que ce dernier :
    - o demeure efficace;
    - o est conforme aux politiques et procédures;
    - o est toujours nécessaire et proportionnel.
- Les politiques et procédures de RPI devraient être examinées régulièrement et mises à jour chaque fois qu'un changement important est apporté au système de RPI. Ces examens devraient être confiés à un tiers indépendant, et il faudrait combler toute lacune ou donner suite à toute préoccupation dans les plus brefs délais.
- Le service de police devrait aussi envisager de publier un rapport annuel sur l'utilisation de son système de RPI décrivant les objectifs du programme, les activités de déploiement et les principales statistiques opérationnelles.

FORMATION

- Le service de police doit fournir une formation appropriée à tous ceux qui ont accès au système.
- La formation initiale et continue devrait comprendre des directives claires sur les rôles, obligations et autres responsabilités.
- Les utilisateurs (policiers, autres employés, fournisseurs de services de l'extérieur) devraient recevoir un exemplaire des politiques et procédures, et signer une entente attestant qu'ils se conformeront aux pratiques établies et respecteront la confidentialité.
- La formation devrait comprendre aussi un exposé des mesures disciplinaires auxquelles s'exposent ceux qui enfreignent les politiques et procédures du service de police.
- Toutes les politiques et procédures applicables devraient être mises à la disposition des policiers, administrateurs de la TI et autres membres du personnel chargés du fonctionnement du programme, ainsi que des fournisseurs de services de l'extérieur.

MÉCANISMES DE PRÉSENTATION DE PLAINTES ET DE RECOURS

- Les politiques et procédures concernant la RPI devraient préciser comment les particuliers peuvent porter plainte et demander à être rayés du système lorsqu'ils sont d'avis que leur plaque d'immatriculation ne devrait pas se trouver sur une liste noire.
- Lorsque l'inscription sur une liste noire concernant un particulier provient d'un autre service de police ou organisme ou d'une autre institution, comme la GRC, le particulier devrait recevoir le nom et les coordonnées du responsable des inscriptions sur la liste noire et de la réception des plaintes ou demandes de recours afin de pouvoir faire retirer cette inscription.
- Le service de police devrait aussi informer le public de son droit de déposer une plainte concernant la protection de la vie privée auprès du CIPVP conformément à la LAIMPVP ou à la LAIPVP, selon le cas.
- Le service de police devrait mettre ces renseignements, ainsi que d'autres renseignements sur ses politiques et procédures de RPI, à la disposition du public sur son site Web.

DEMANDES D'ACCÈS À L'INFORMATION

- Le service de police doit établir un processus afin de pouvoir répondre aux demandes d'accès dans le délai prévu par la loi.
- Le service de police devrait consulter son coordonnateur de l'accès à l'information et de la protection de la vie privée pour obtenir des conseils sur la façon de répondre aux demandes d'accès à l'information.
- Le service de police qui refuse une demande d'accès à l'information doit informer l'auteur de la demande de son droit d'interjeter appel au CIPVP.

Document d'orientation sur l'utilisation de systèmes de reconnaissance des plaques d'immatriculation par les services de police

Information and Privacy Commissioner of Ontario
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

Site web : www.ipc.on.ca/fr/
Téléphone : 416 326-3333
Courriel : info-fr@ipc.on.ca

Décembre 2024