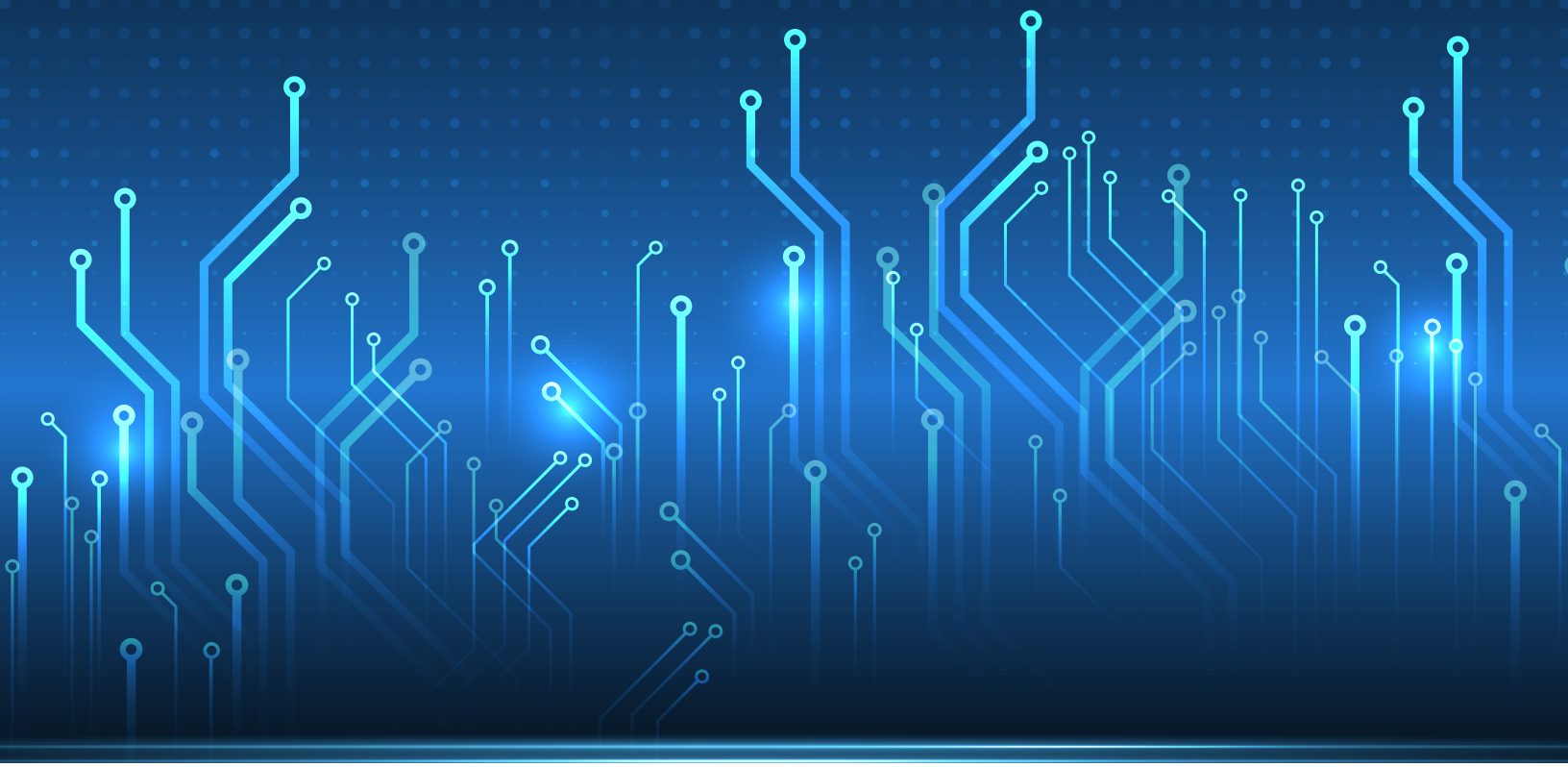
GRC·RCMP

GENDARMERIE ROYALE DU CANADA • ROYAL CANADIAN MOUNTED POLICE

Programme national d'intégration de la technologie

Plan de transparence : *Aperçu des technologies opérationnelles*



Gendarmerie royale du Canada
Royal Canadian Mounted Police

Canada

Table des matières

Introduction

Grâce aux progrès rapides des télécommunications au cours des dernières années, nous profitons des nombreux avantages offerts par un monde moderne connecté. Cependant, les mêmes technologies qui nous facilitent la vie peuvent aussi être exploitées par les criminels pour planifier et commettre des crimes, ainsi que pour dissimuler toute preuve de leurs activités criminelles. Pour s'attaquer à ce problème, la Gendarmerie royale du Canada (GRC) doit constamment examiner la façon dont les technologies nouvelles et émergentes peuvent servir à lutter contre la criminalité et à assurer la sécurité des Canadiens et des Canadiennes.

En 2021, le Programme national d'intégration de la technologie (PNIT) a été établi pour garantir l'utilisation responsable des technologies opérationnelles par la GRC et pour encourager une plus grande transparence publique relativement à ces technologies. Le *Plan de transparence : Aperçu des technologies opérationnelles* est la première publication du PNIT sur son travail.

Qu'est-ce qu'une technologie opérationnelle?

Tout outil, technique, dispositif, logiciel, application ou ensemble de données fondé sur la technologie et utilisé à l'appui des enquêtes de la GRC ou de la collecte de renseignements.

Le *Plan de transparence* donne un aperçu du mandat du PNIT et des principes clés de l'utilisation responsable des technologies opérationnelles par la GRC. Il précise aussi les types de technologies opérationnelles évaluées par le PNIT aux fins d'utilisation par la GRC, ainsi que certaines tendances liées à l'utilisation de ces technologies. Le *Plan de transparence* décrit aussi plus en détail comment et pourquoi la GRC utilise les trois principales technologies opérationnelles suivantes, et précise les situations où elles peuvent être utilisées, les informations qu'elles permettent de recueillir, et les autorités judiciaires qui régissent leur utilisation :

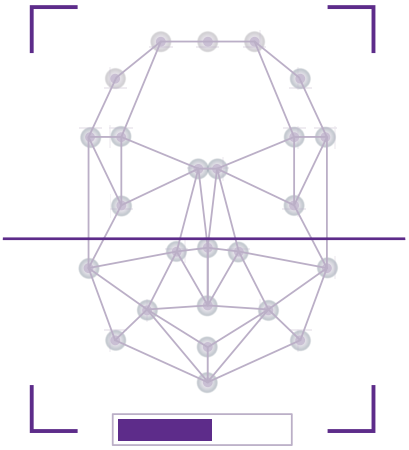
1. Outils d'enquête embarqués;
2. Simulateurs de station cellulaire;
3. Systèmes d'aéronefs télépilotés (communément appelés drones).

La GRC reconnaît que l'utilisation des technologies opérationnelles devrait concilier les besoins de l'application de la loi et les questions de respect de

la vie privée et d'éthique qui y sont associées. Bien qu'il ne soit pas toujours possible d'indiquer exactement quand et comment certaines technologies opérationnelles sont utilisées, puisque cela pourrait nuire à leur efficacité, le PNIT favorise la transparence comme un facteur clé pour maintenir la confiance du public dans l'utilisation responsable de ces technologies par la GRC.

Le *Plan de transparence* est la première étape du PNIT pour renseigner la population sur l'utilisation responsable des technologies opérationnelles par la GRC. Les prochaines étapes comprendront la publication proactive de sommaires sur les évaluations de certaines technologies opérationnelles par le PNIT. Ces efforts cadrent avec la promesse de la GRC d'améliorer la transparence dans le cadre du *Plan stratégique Vision150 et au-delà*, l'Engagement de transparence en matière de sécurité nationale du gouvernement du Canada[1], ainsi que les obligations de la GRC de publier des résumés des évaluations des facteurs relatifs à la vie privée (EFVP) conformément à la *Directive sur l'évaluation des facteurs relatifs à la vie privée* du Secrétariat du Conseil du Trésor[2].

Programme national d'intégration des technologies (PNIT)



Le PNIT a été établi en 2021 à la suite de l'enquête menée par le Commissariat à la protection de la vie privée (CPVP) sur l'utilisation par la GRC de la technologie de reconnaissance faciale Clearview AI[3]. Le CPVP a conclu que Clearview AI avait enfreint les lois fédérales canadiennes sur la protection de la vie privée en créant une banque de données renfermant des milliards d'images capturées sur divers sites Web sans le consentement des personnes figurant sur les images. Par conséquent, le CPVP a jugé que la collecte de renseignements personnels par Clearview AI pour la GRC n'était pas conforme aux exigences de la *Loi sur la protection des renseignements personnels*, puisque ces renseignements n'avaient pas été recueillis légalement. Ces constatations ont aussi mis en évidence des préoccupations liées à la transparence et de responsabilité, puisque la GRC n'avait pas de procédures établies pour veiller à ce que les pratiques de collecte de renseignements personnels par des fournisseurs de services tiers respectent les lois canadiennes en matière de protection de la vie privée.

En réponse à l'enquête et aux constatations du CPVP, la GRC a créé le PNIT. Le PNIT a pour principal but de centraliser et d'uniformiser le processus utilisé par la GRC pour identifier et évaluer son utilisation des technologies opérationnelles et en assurer le suivi.

Le PNIT est responsable d'effectuer des évaluations approfondies des technologies opérationnelles nouvelles et existantes, pour s'assurer qu'elles sont nécessaires sur le plan opérationnel; présentent un avantage clair pour le public; et respectent les normes juridiques, éthiques, de confidentialité et qu'ils sont établies dans les politiques. Les technologies opérationnelles qui portent atteinte à la vie privée ou qui contiennent de l'intelligence artificielle reçoivent la plus grande priorité.

Selon la politique de la GRC, les secteurs de programme de la GRC doivent consulter le PNIT lorsqu'ils envisagent de recourir à des technologies opérationnelles ou à de nouveaux ensembles de données qui comprennent la collecte ou l'utilisation de renseignements personnels. Une collaboration étroite avec les secteurs de programme de la GRC est nécessaire pour assurer le respect des exigences d'évaluation des technologies opérationnelles.

En outre, un thème central des études récentes réalisées par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes concernant l'utilisation de technologies par la police était la nécessité d'accroître la transparence et la reddition de comptes[4 5]. En plus de réaliser des évaluations approfondies tel qu'il est décrit ci-dessus, le PNIT est aussi responsable d'informer le public de l'utilisation des technologies opérationnelles par la GRC.

Mandat

Le PNIT est responsable d'évaluer de façon approfondie et objective les technologies opérationnelles avant qu'elles soient utilisées par la GRC. Cela comprend les éléments et activités clés suivants :

- Mettre en place des procédures standard pour l'évaluation et l'adoption des technologies opérationnelles;
- Évaluer l'efficacité des nouvelles technologies opérationnelles;
- Veiller à ce que les techniques de collecte de données soient conformes à la loi et à l'éthique;
- Veiller à ce que les technologies opérationnelles soient utilisées lorsqu'ils sont nécessaires;
- Assurer la surveillance et le suivi des technologies utilisées par la GRC et en faire rapport;
- Informer la population de l'utilisation par la GRC des technologies opérationnelles.






Utilisation responsable des technologies opérationnelles – principes clés

Le PNIT évalue les technologies opérationnelles selon 10 principes clés, en collaboration avec plusieurs partenaires internes. Cela permet de veiller à ce que ces technologies soient utilisées de façon responsable, uniquement lorsqu'il est nécessaire, et de façon proportionnelle; c'est-à-dire que leur utilisation doit être directement liée à un objectif de sécurité publique clairement défini. Le PNIT s'assure que l'utilisation de ces technologies par la GRC respecte des conditions relatives à la responsabilisation, au respect de la vie privée et à la transparence.

Les principes suivants sont conformes au Cadre stratégique pour la technologie de l'Association internationale des chefs de police [en anglais seulement], pour une utilisation responsable et efficace des technologies policières[6].

1. Responsabilité

- La structure de responsabilisation pour les technologies opérationnelles de la GRC devrait être clairement établie et transparente, tout en protégeant les éléments sensibles.
- Les rôles et responsabilités des décideurs et des opérateurs de la GRC devraient être déterminés, consignés et conformes à l'utilisation des technologies opérationnelles.

2. Transparence

- Pour que la population ait confiance en la façon dont la GRC utilise les technologies opérationnelles, et pour que les citoyens comprennent l'utilisation légitime des technologies policières, il faut faire preuve de transparence.
- La GRC mettra en place de nouveaux moyens d'optimiser la transparence et de tenir davantage de dialogues bilatéraux avec la population canadienne

Le PNIT travaille en étroite collaboration avec des experts en la matière des sous-directions et services de la GRC suivants :

- Accès à l'information et protection des renseignements personnels
- Groupe des services juridiques
- Sécurité ministérielle - Sécurité des technologies de l'information et des communications
- Programme de gestion de la collectivité des technologies de l'information
- Programme de gestion des dossiers techniques
- Gestion des relations et des portefeuilles clients

et les principales parties prenantes à propos des technologies opérationnelles, notamment en sollicitant les commentaires de la population sur les politiques opérationnelles.

3. Protection des renseignements personnels

- Les technologies opérationnelles peuvent être utilisées pour la collecte, l'utilisation, l'analyse et la divulgation légales de renseignements personnels afin de mener les activités de la GRC et d'atteindre les objectifs de celle-ci[7].
- Les technologies opérationnelles devraient être assujetties à une analyse et à une évaluation pour assurer une protection adéquate des renseignements personnels.

4. Spécificité

- Les technologies opérationnelles devraient être adaptées aux besoins et conformes à des objectifs d'application de la loi et à des exigences opérationnelles clairs et explicables.
- Les exigences associées à une technologie opérationnelle devraient présenter toutes les considérations légales, politiques et opérationnelles afin de veiller à ce que le déploiement de la technologie et son utilisation soient conformes aux lois et répondent à un objectif policier légitime.

5. Exactitude

- Les technologies opérationnelles devraient s'appuyer sur des données opérationnelles exactes, complètes et à jour pour soutenir les activités et les décisions de la GRC.
- Des attributs de qualité des données rigoureux devraient être associés aux technologies opérationnelles de la GRC, par exemple des procédures et des mécanismes techniques qui assurent l'exactitude des données, y compris l'utilisation pertinente, cohérente et opportune des informations opérationnelles.

6. Formation

- Une formation initiale ainsi que de la formation continue doivent être offertes pour assurer une utilisation responsable des technologies opérationnelles par les membres de la GRC et limiter le risque d'utilisation inappropriée et d'inconduite.
- Il devrait y avoir pour les technologies opérationnelles des protocoles de formation appropriés et exhaustifs pour tous les utilisateurs autorisés (formations de base et avancée), et la formation devrait améliorer le savoir-faire en matière de données dans ce domaine au sein de la GRC.

7. Incidence

- L'utilisation des technologies opérationnelles par la GRC peut avoir une incidence disproportionnée sur certains groupes et populations, comme les victimes de crimes. L'ampleur de cette incidence dépend des capacités des technologies opérationnelles, de leur utilisation, ampleur et portée, et d'autres facteurs.
- La GRC doit évaluer exhaustivement l'incidence sur les Canadiens des technologies opérationnelles qu'elle utilise, notamment toute incidence disproportionnée sur certains groupes, personnes ou communautés[8].

8. Restrictions

- L'utilisation des technologies opérationnelles par la GRC devrait avoir des liens clairs avec les lois habilitantes ou la politique, et être assortie des mesures de protection pour en définir le champ d'application autorisé.
- La GRC doit prévoir des restrictions et des techniques d'atténuation pour les technologies opérationnelles, notamment le recours à ces technologies pour les crimes graves uniquement dans les cas appropriés.

9. Sécurité

- La GRC est responsable de la sécurité et de la protection des renseignements qu'elle recueille au moyen de technologies opérationnelles, en particulier les renseignements personnels.
- Des mesures de gestion et de sécurité des renseignements devraient être associées aux technologies opérationnelles afin de rendre leur utilisation sécuritaire, notamment au chapitre de la confidentialité, de l'intégrité et de la disponibilité des données.

10. Évaluation

- Pour inspirer la confiance de la population envers les technologies opérationnelles, il est essentiel que ces dernières puissent faire l'objet d'évaluations, de vérifications et d'audits. Cela est aussi essentiel à l'évaluation et à l'amélioration continues de l'utilisation de ces technologies par la GRC.
- La GRC devrait suivre et évaluer régulièrement le rendement de ses technologies opérationnelles, et gérer ces dernières de façon à permettre leur évaluation, examen et audit par des organisations externes.

Le saviez-vous?

Le PNIT collabore étroitement avec la Sous-direction de l'accès à l'information et de la protection des renseignements personnels de la GRC pour évaluer l'incidence des technologies opérationnelles sur la protection de la vie privée.

Cela comprend la collecte, l'utilisation, la conservation et la divulgation légales de renseignements personnels dans le respect de la *Loi sur la protection des renseignements personnels*.

Depuis 2019, la GRC s'efforce d'adopter une approche plus moderne pour l'accès à l'information et la protection des renseignements personnels, notamment en améliorant la transparence, en procédant à des EFVP et en prenant d'autres mesures.

Pour en savoir plus, consultez la Stratégie de modernisation de la GRC – Accès à l'information et protection des renseignements personnels.

Aperçu des technologies opérationnelles

Les technologies opérationnelles jouent un rôle essentiel dans les services de police modernes. Elles sont utilisées dans la lutte contre la criminalité, les enquêtes, la protection des enfants et d'autres groupes vulnérables, la collecte d'éléments de preuve, l'amélioration de l'analyse de données, la responsabilisation accrue de la police, et la réalisation d'objectifs d'application de la loi et de sécurité publique.

Pour suivre l'évolution des criminels et assurer la sécurité du public, la GRC doit continuellement s'adapter, innover et utiliser des technologies nouvelles et émergentes. Parallèlement, ces technologies doivent être utilisées de façon responsable et appropriée. Lorsque des technologies nouvelles ou potentiellement invasives sont utilisées, il faut tenir compte rigoureusement des facteurs juridiques, éthiques, liés au respect de la vie privée et liés à l'intérêt public.

Les technologies opérationnelles évaluées par le PNIT appartiennent à une ou à plusieurs des catégories suivantes :

1. **Technologie algorithmique** : Technologies guidées par des algorithmes qui permettent aux organismes d'application de la loi de tirer des déductions du traitement de données en masse, dans le but de « prédire » les activités illégales potentielles en dégageant des tendances. Ces technologies comprennent les logiciels de reconnaissance des plaques d'immatriculation et d'autres outils qui utilisent des algorithmes et l'apprentissage machine.
2. **Intelligence artificielle** : Toute application logicielle qui utilise des algorithmes d'intelligence artificielle pour effectuer des tâches précises ou résoudre des problèmes. Les outils d'intelligence artificielle peuvent servir dans divers contextes pour automatiser des tâches, analyser des données, et améliorer la prise de décisions.
3. **Simulateurs de station cellulaire** : Imitent une station de base; utilisés pour identifier les appareils cellulaires à proximité. Recueillent les numéros d'identification seulement; n'interceptent pas de communications privées. Parfois appelés capteurs d'IMSI (*International Mobile Subscriber Identification*, ou numéro d'identité internationale d'abonné mobile).
4. **Caméras de sécurité, vidéo et surveillance** : Système ou dispositif vidéo électronique qui surveille des lieux publics en vue de déceler et d'enregistrer des événements criminels ou toute autre menace pour la sécurité du public. Cette catégorie comprend les caméras d'intervention et les services de registre de caméras.
5. **Bases de données sur les groupes criminels (jeu de données)** : Ressources d'enquête permettant de maintenir des renseignements cohérents et à jour concernant des groupes criminels et des gangs de rue.
6. **Outils d'analyse des cryptomonnaies** : Effectuent des activités de recherche d'adresses de cryptomonnaies dans la chaîne de blocs, ainsi que d'autres sources de données publiques sur Internet, comme les informations sur les transactions en cryptomonnaie.
7. **Outils judiciaires numériques** : Logiciels et matériel utilisés pour accéder à des informations trouvées sur des appareils électroniques, et extraire et traiter ces informations. Dans certains cas, le logiciel peut aussi faciliter l'extraction de l'information de services en nuage.
8. **Drones et systèmes de détection de drones** : La GRC désigne ces appareils, communément appelés drones, sous le nom de systèmes d'aéronefs télépilotés (SATP). Les systèmes de détection de drones sont utilisés pour identifier les SATP n'appartenant pas à la GRC.
9. **Logiciels de reconnaissance faciale** : La reconnaissance faciale est une technologie numérique utilisée pour comparer les images obtenues au cours d'enquêtes criminelles avec des photographies de personnes connues légalement obtenues.
10. **Dispositifs du système de localisation GPS** : Appareils capables de déterminer ou d'estimer l'emplacement géographique d'un appareil ou d'un objet à localiser.
11. **Infrastructure de gestion d'attribution Internet** : Les activités sur Internet et les traces qu'elles laissent derrière elles créent souvent des données ou des « empreintes numériques ». Ces outils aident à recenser et à interpréter les données, qui peuvent comprendre des adresses IP, des identifiants de publicité, et d'autres données générées par des réseaux et des dispositifs.
12. **Services de regroupement du contenu média** : Plateformes logicielles qui font des recherches dans des milliers de sources d'informations publiques sur Internet, et avisent les utilisateurs de leur existence. Ces alertes peuvent aussi comprendre un lien vers la source d'information originale sur Internet, ainsi que le moment où cette information a été affichée sur Internet.

13. **Outils d'enquête embarqués (OEE)** : Programmes informatiques répondant à la définition figurant à l'article 342.1(2) du *Code criminel* qui sont installés sur un dispositif informatique cible pour permettre la collecte d'éléments de preuve électronique discrète à distance.
14. **Renseignements de sources ouvertes** : Collecte et analyse de données recueillies de sources ouvertes (Internet) en vue de produire des renseignements susceptibles de donner lieu à une action. Ces renseignements sont principalement utilisés dans le domaine de l'application de la loi, de la sécurité publique et de la sécurité nationale aux fins de connaissance de la situation et pour les besoins de la preuve
15. **Outils d'analyse de réseaux sociaux** : Outils de traitement de l'information des plateformes de réseaux sociaux qui permettent aux policiers de découvrir des informations pertinentes pour leurs enquêtes et pour des raisons de sécurité publique.

À ce jour, le PNIT a terminé l'évaluation de 28 technologies appartenant à ces catégories.

Trois technologies opérationnelles utilisées par la GRC

Le PNIT surveille de près plusieurs variables associées à l'utilisation responsable des trois technologies opérationnelles potentiellement invasives suivantes :

1. Outils d'enquête embarqués;
2. Simulateurs de station cellulaire;
3. Systèmes d'aéronefs télépilotés.

Ceci ne s'agit pas d'une liste exhaustive de toutes les technologies opérationnelles utilisées par la GRC. Dans les prochaines publications axées sur la transparence, le PNIT traitera d'une plus vaste gamme de technologies opérationnelles utilisées par la GRC, dont les caméras d'intervention , le système de reconnaissance automatique des plaques d'immatriculation[10], les outils de renseignements de sources ouvertes, la reconnaissance faciale et d'autres technologies clés.

Outils d'enquête embarqués

De quoi s'agit-il?

Un outil d'enquête embarqué est un programme informatique qui peut être installé dans un appareil numérique pour permettre à la police de recueillir secrètement des preuves électroniques. On a seulement recours à ces outils dans les enquêtes relatives aux crimes graves ou à la sécurité nationale, et seulement après avoir obtenu une autorisation judiciaire.

Après avoir obtenu une autorisation judiciaire, la GRC utilise des outils d'enquête embarqués afin d'obtenir en toute légalité des communications privées et d'autres informations des appareils ciblés avant qu'elles ne soient chiffrées, ou après qu'elles ont été déchiffrées sur les appareils des suspects, puisque le chiffrement rend les informations inintelligibles.

Ainsi, les renseignements peuvent être obtenus dans un format clair et intelligible (texte en clair) et utilisés à des fins d'application de la loi[11].

Pourquoi sont-ils utilisés?

Dans le passé, le recours par les forces de l'ordre à l'écoute électronique judiciairement autorisée était une technique d'enquête relativement simple. Avec l'évolution des technologies cellulaires et des communications numériques, cette activité policière est de plus en plus complexe et poussée sur le plan technique[12 13].

L'utilisation du chiffrement par les criminels complique l'interception légale des communications par la police. Le chiffrement est un élément essentiel de la cybersécurité et de la prévention de la criminalité, car il protège les données contre l'accès et l'utilisation non autorisés. Cependant, lorsque les criminels utilisent le chiffrement et d'autres méthodes assurant un anonymat en ligne, cela leur permet de planifier et de mener des activités criminelles graves, comme le terrorisme, le crime organisé, la criminalité financière, l'exploitation sexuelle d'enfants en ligne et d'autres types de cybercrimes. Les criminels se servent de ces moyens technologiques pour échapper aux forces de l'ordre et cibler les victimes, dont les citoyens et les organisations au Canada.

Comment fonctionnent-ils?

Les capacités techniques d'un outil d'enquête embarqué varient et dépendent de l'objectif d'application de la loi et de la portée de l'autorisation judiciaire, qui doit être obtenue avant qu'un tel outil ne soit utilisé. Les capacités techniques peuvent comprendre l'interception de communications, la collecte et l'entreposage de données, les captures d'écrans et l'enregistrement de frappe, ou l'activation des fonctions de microphones et de caméras.

Principales caractéristiques des outils d'enquête embarqués pour la collecte de preuves

- Interception de communications en ligne
- Collecte et entreposage de données
- Captures d'écrans
- Enregistrement de frappe
- Activation des fonctions de microphones et de caméras

Quand sont-ils utilisés?

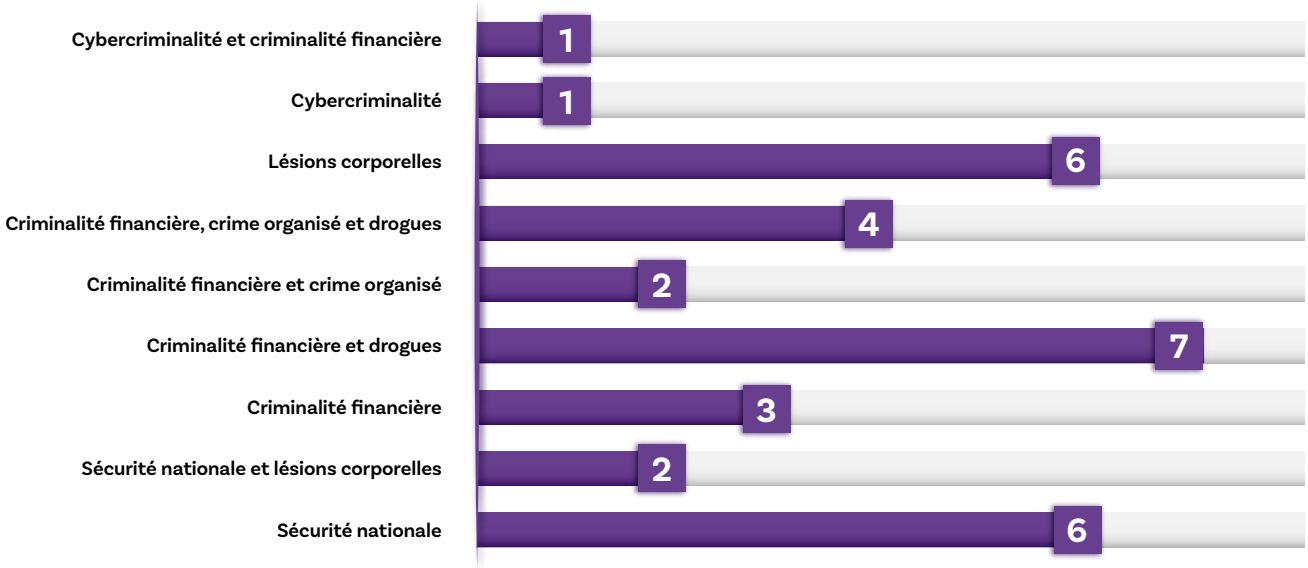
La GRC n'a recours aux outils d'enquête embarqués que lors d'enquêtes sur des activités criminelles graves, comme celles liées au crime organisé, à la sécurité nationale et au terrorisme ou à d'autres crimes graves. Cette technique est seulement utilisée lorsque d'autres moyens de collecte de preuve se sont révélés inefficaces.

De 2017 à 2022, la GRC a recouru à ces outils pour 32 enquêtes criminelles ciblant 49 dispositifs en tout. Pendant la même période, la GRC a consigné plus de 13 millions d'incidents nécessitant l'intervention de la police[14] [15].

Le tableau ci-dessous présente une ventilation du recours par la GRC à des outils d'enquête embarqués, par catégorie d'infraction criminelle, établie en fonction des déploiements entre 2017 et 2022. Comme illustré, les catégories « sécurité nationale » (comprend les infractions liées au terrorisme), « lésions corporelles », « criminalité financière » et « infractions liées aux drogues » forment la majorité des enquêtes criminelles dans le cadre desquelles des outils d'enquête embarqués ont été utilisés. Dans la plupart des cas, les enquêtes dans le cadre desquelles des outils d'enquête embarqués ont été utilisés portaient sur plusieurs infractions criminelles.

Diagramme 1 : Infractions criminelles ayant entraîné le recours à des outils d'enquête embarqués

Infractions criminelles ayant entraîné le recours à des outils d'enquête embarqués
Utilisation par la GRC de 2017 à 2022 (total de 32 enquêtes)



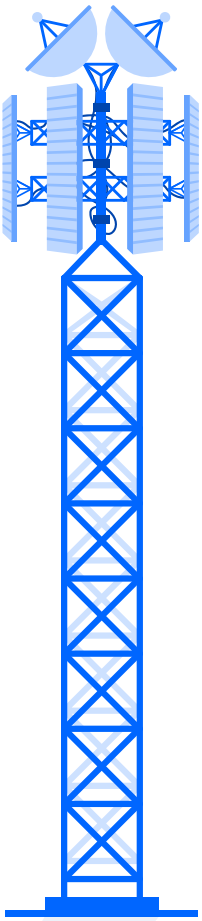
L'utilisation par la GRC d'outils d'enquête embarqués est conforme à ses fonctions de protection du public et de prévention du crime, décrites à l'article 18 de la *Loi sur la Gendarmerie royale du Canada*. Les exigences à respecter pour les autorisations d'intercepter une communication privée (mandat d'interception) sont indiquées à la partie VI du *Code criminel*.

Le saviez-vous?

La *Charte canadienne des droits et libertés* (la Charte) protège les Canadiens contre les fouilles, perquisitions et saisies illégales. Une communication privée comprend une attente raisonnable de respect de la vie privée, et pour cette raison, l'interception de communications privées est considérée comme une fouille (et une saisie) au sens de l'article 8 de la Charte.

La GRC a recours aux technologies opérationnelles, et recueille des données personnelles dans le respect de la Charte et des attentes en matière de vie privée, y compris les exigences du *Code criminel*, des pouvoirs procéduraux et des autorisations judiciaires visant la collecte d'éléments de preuve, comme les mandats généraux, les mandats d'interception pour la surveillance électronique, ainsi que les mandats spécialisés, les ordonnances de production et les autres instruments juridiques.

Pour demander un mandat d'interception des communications, la police doit expliquer au juge si d'autres méthodes d'enquête ont été essayées et ont échoué, ou pourquoi ces méthodes ont vraisemblablement peu de chance de succès. Le type de mandat obtenu dépend notamment de l'information à obtenir, de l'utilisation prévue des outils et du consentement d'une partie. Par exemple, la collecte de communications antérieures d'un suspect visé par une enquête et la collecte de futures communications exigent différents types d'autorisations judiciaires. La plupart du temps, pour pouvoir utiliser des outils d'enquête embarqués, la GRC doit obtenir plusieurs mandats, qui sont d'une durée limitée et soumis à d'autres restrictions.



La seule exception à l'obtention d'une autorisation judiciaire préalable est lorsque l'urgence de la situation rend cela difficile, comme le prévoit l'article 188 du *Code criminel*. Il s'agit notamment de situations urgentes où l'action rapide des policiers est requise pour prévenir un danger imminent pour une personne, une menace pour la vie, des dommages importants à des biens, ou la destruction potentielle d'éléments de preuve . À ce jour, la GRC n'a jamais eu recours à l'urgence de la situation pour déployer un outil d'enquête embarqué, et a toujours obtenu une autorisation judiciaire préalable.

Les données recueillies à l'aide d'outils d'enquête embarqués sont chiffrées et entreposées de façon sécuritaire par la GRC et protégées par des mesures rigoureuses de contrôle d'accès basées sur les politiques et lignes directrices du gouvernement du Canada et de la GRC en matière de gestion de l'information et de traitement des éléments de preuve.

Simulateurs de station cellulaire

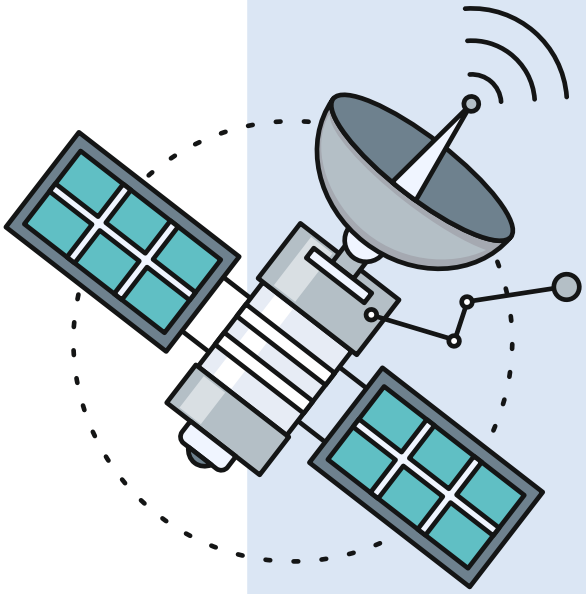
De quoi s'agit-il?

Un simulateur de station cellulaire est un dispositif électronique qui, lorsqu'il est activé, imite le fonctionnement d'une station cellulaire afin que tous les téléphones mobiles et autres appareils cellulaires à proximité s'y connectent. Les identifiants alphanumériques uniques[18] obtenus de ces appareils peuvent être utilisés pour suivre l'emplacement des appareils visés, ou par la suite pour identifier le propriétaire de l'appareil.

Pourquoi sont-ils utilisés?

La GRC peut utiliser des simulateurs de station cellulaire dans le cadre d'enquêtes à priorité élevée liées à la sécurité nationale, aux crimes graves, au crime organisé et à d'autres infractions au *Code criminel* qui mettent en péril la sécurité des Canadiens. Cette technologie peut également être utilisée dans des situations urgentes, comme en cas d'enlèvement ou de disparition de personnes[19].

Sauf dans des situations urgentes, la GRC obtient une autorisation judiciaire avant d'utiliser un simulateur de station cellulaire[20]. Il s'agit dans la plupart des cas d'un mandat pour un enregistreur de données de transmission et d'un mandat de localisation. Conformément à la *Loi sur la radiocommunication*, la GRC obtient aussi une lettre d'autorisation d'Innovation, Sciences et Développement économique Canada pour l'utilisation de simulateurs de station cellulaire au Canada[21].



Données de transmission

Le *Code criminel* définit les données de transmission comme les données qui, à la fois :

a) concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication;

b) soit sont transmises pour identifier, activer ou configurer un dispositif, notamment un programme d'ordinateur au sens du paragraphe 342.1(2) du *Code criminel* [Utilisation non autorisée d'ordinateur], en vue d'établir ou de maintenir l'accès à un service de télécommunication afin de rendre possible une communication, soit sont produites durant la création, la transmission ou la réception d'une communication et indiquent, ou sont censées indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication;

c) ne révèlent pas la substance, le sens ou l'objet de la communication.

Comment fonctionnent-ils?

Les simulateurs de station cellulaire ne permettent pas à la GRC d'intercepter les communications privées, comme le contenu des communications audio, les messages textes ou les courriels. Ils ne sont utilisés que pour consigner les identificateurs alphanumériques uniques associés aux appareils cellulaires. La GRC doit obtenir une autre autorisation judiciaire pour avoir accès aux renseignements personnels de l'abonné associé à un appareil mobile utilisé par un suspect visé par une enquête.

Toutes les données recueillies à l'aide de simulateurs de station cellulaire sont entreposées de façon sécuritaire, conformément aux politiques et lignes directrices applicables du gouvernement du Canada et de la GRC.

Le saviez-vous?

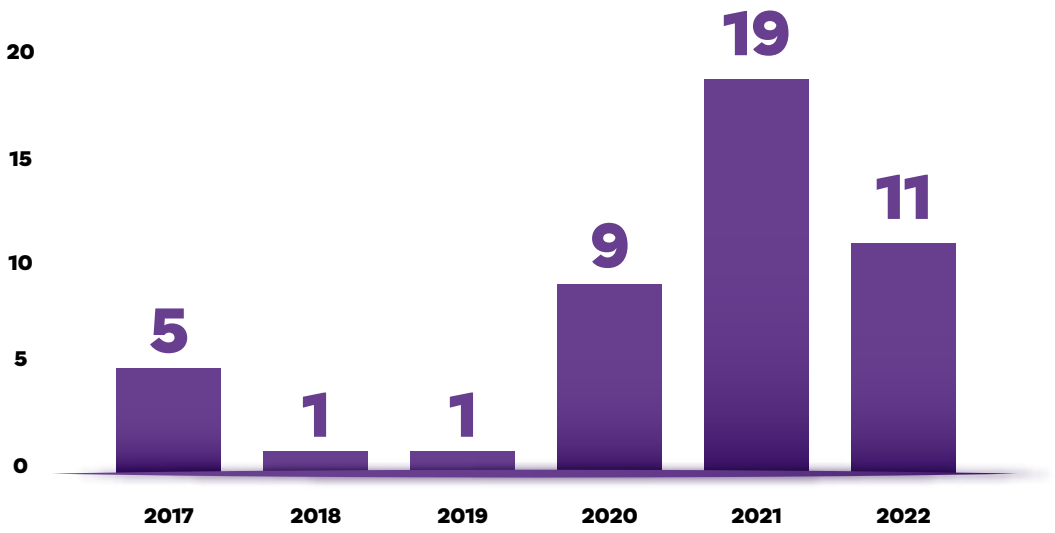
En situation d'urgence, comme en cas d'enlèvement, où une victime pourrait être exposée à un danger immédiat et qu'une action rapide est requise pour prévenir une menace pour la vie, des dommages importants à des biens, ou la destruction potentielle d'éléments de preuve, la GRC peut utiliser des simulateurs de station cellulaire sans obtenir d'autorisation judiciaire préalable. Dans ces cas, une autorisation judiciaire serait demandée dans les plus brefs délais, en expliquant la situation d'urgence.

Quand sont-ils utilisés?

De 2017 à 2022, la GRC a eu recours à un simulateur de station cellulaire dans 46 enquêtes. Le diagramme suivant présente l'utilisation par la GRC de cette technologie, ventilée par année.

Diagramme 2 : Utilisation de simulateurs de station cellulaire

Utilisation de simulateurs de station cellulaire par la GRC



Pour en savoir plus sur l'utilisation de simulateurs de station cellulaire par la GRC, voir le rapport de 2017 du Commissariat à la protection de la vie privée du Canada, intitulé *Les simulateurs de sites cellulaires utilisés par la GRC ne peuvent pas intercepter les communications privées*.

Systèmes d'aéronefs télépilotés

De quoi s'agit-il?

Comme ils sont très agiles et peuvent être déployés rapidement, les systèmes d'aéronefs télépilotés (SATP), communément appelés drones, sont utilisés pour la surveillance aérienne. Ces systèmes sont équipés de caméras infrarouges ou électro-optiques[22]. Ils sont utilisés pour soutenir diverses opérations critiques de la GRC, comme les lieux de crimes graves, les missions de recherche et sauvetage, les lieux d'accidents de la route ou les situations à risque élevé nécessitant l'intervention d'un Groupe tactique d'intervention de la GRC[23].

Le Programme des systèmes d'aéronef télépiloté de la GRC a réalisé une EFVP pour s'assurer de sa conformité aux lois et règlements canadiens en matière de protection de la vie privée[24]. L'EFVP énonce des protocoles rigoureux pour la manipulation des données recueillies par un SATP, et met l'accent sur la protection des renseignements personnels. L'utilisation d'un SATP se concentre particulièrement sur le soutien aux enquêtes, et les données recueillies sont intégrées de façon sécuritaire aux systèmes de la GRC, ou supprimées conformément aux calendriers de conservation des données.

Pourquoi sont-ils utilisés?

Lors d'une intervention à l'extérieur (p. ex., opération de recherche et sauvetage pour retrouver une personne vulnérable), les SATP permettent aux policiers de mieux comprendre la situation, car ils leur fournissent des renseignements importants et permettent de recueillir de meilleurs éléments de preuve. L'utilisation de SATP dans les environnements à risque élevé permet également aux policiers de moins s'exposer aux risques dans certaines situations.

Le saviez-vous?

Tous les SATP de la GRC sont enregistrés auprès de Transports Canada et portent un numéro d'enregistrement unique.

Seuls des pilotes de la GRC qualifiés et certifiés contrôlent les SATP, conformément aux exigences présentées dans le Programme des systèmes d'aéronef télépiloté de la GRC et au *Règlement de l'aviation canadien* de Transports Canada.

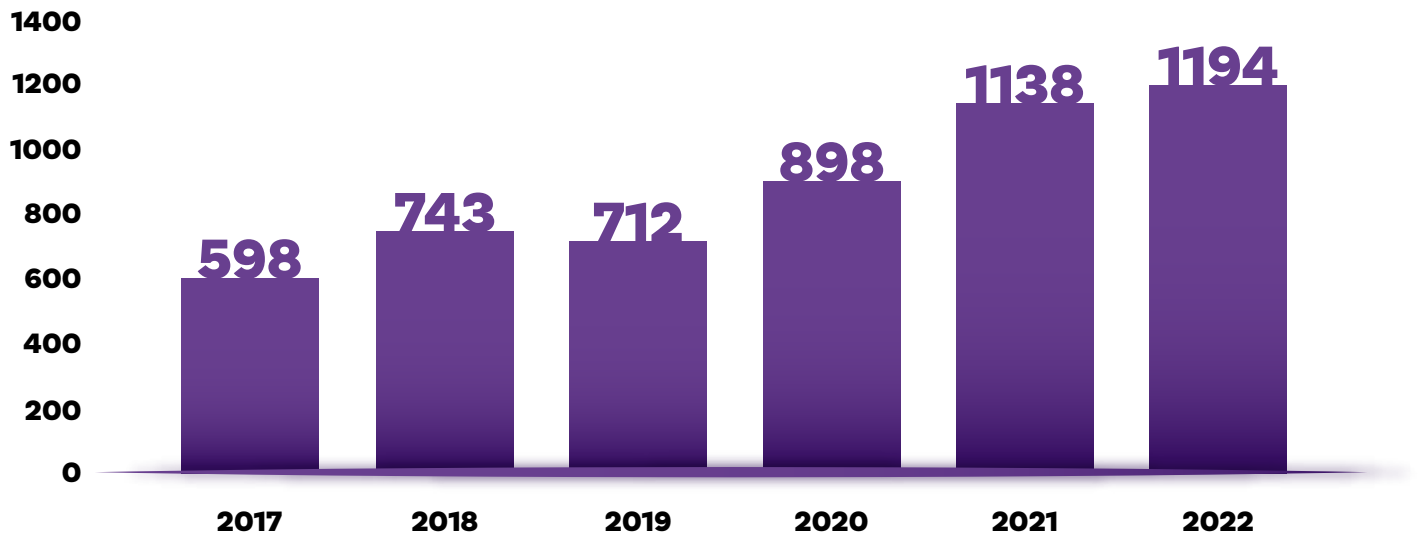
Comment fonctionnent-ils?

L'utilisation par la GRC de SATP est conforme à ses fonctions de protection du public et de prévention du crime, décrites à l'article 18 de la *Loi sur la Gendarmerie royale du Canada*. L'exigence visant une autorisation judiciaire préalable dépend du contexte opérationnel et de l'utilisation prévue. Les activités de surveillance aérienne qui portent atteinte à l'attente raisonnable en matière de vie privée exigent l'obtention d'une autorisation judiciaire préalable. Par exemple, un mandat serait nécessaire pour utiliser un SATP pour filmer la cour arrière d'une résidence privée associée à un suspect visé par une enquête.

Le Programme des systèmes d'aéronef télépiloté de la GRC dispose d'une flotte de 399 SATP enregistrés et de près de 300 pilotes qualifiés et certifiés à l'échelle du Canada. Le diagramme ci-dessous illustre l'utilisation de SATP par la GRC entre 2017 et 2022.

Diagramme 3 : Nombre de vols effectués par des SATP de la GRC, par année

Systèmes d'aéronefs télépilotés de la GRC : vols opérationnels par année

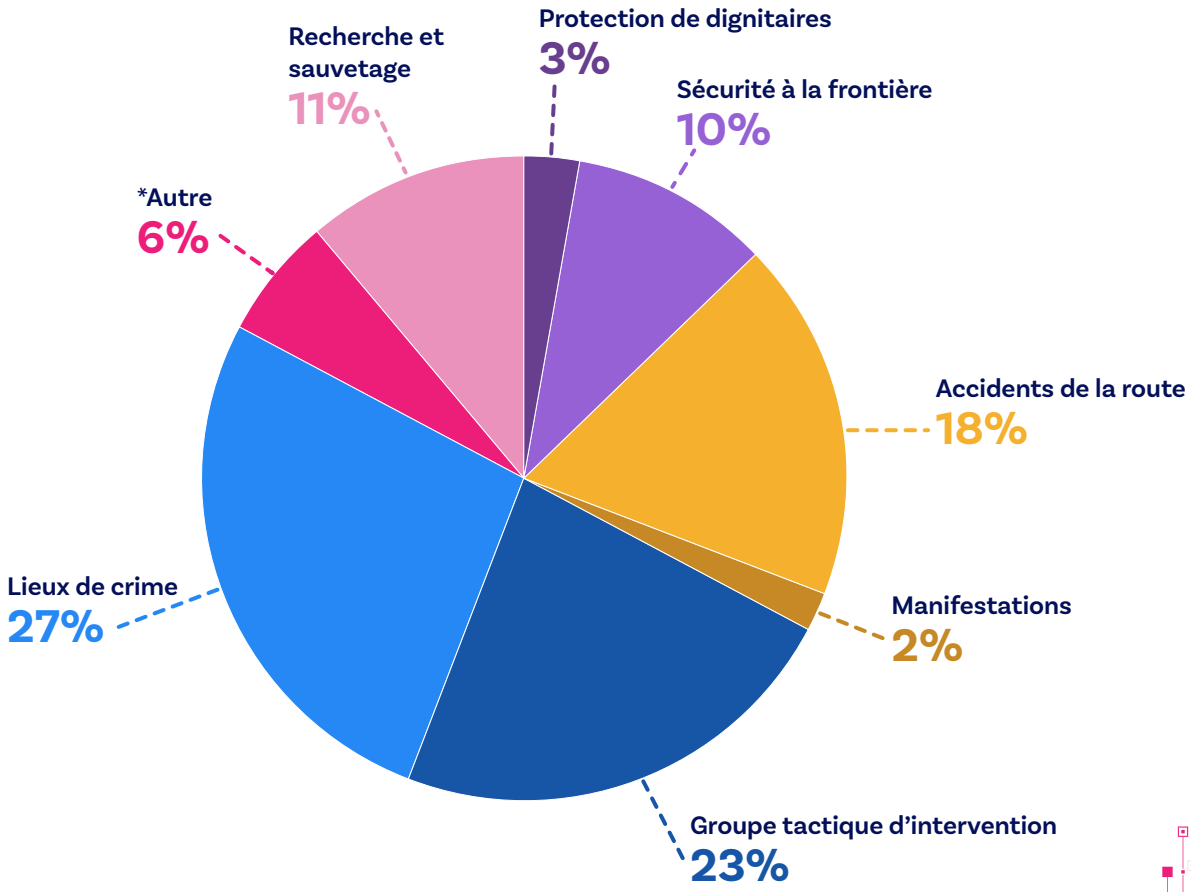


Quand sont-ils utilisés?

Le Programme des SATP de la GRC a pris de l'ampleur au cours des dernières années, 1 194 missions opérationnelles ayant été consignées en 2022. Parmi ces missions, on compte des enquêtes sur un lieu de crime, des opérations du Groupe tactique d'intervention, des enquêtes sur des lieux d'accidents de la route, la sécurité à la frontière, des opérations de recherche et sauvetage et d'autres activités policières. Les données recueillies grâce aux SATP sont évaluées afin de déterminer si elles sont de nature probante, administrative ou éphémère. Toutes les informations sont conservées conformément aux politiques et lignes directrices du gouvernement du Canada et de la GRC en matière de gestion de l'information et de traitement des éléments de preuve. À l'heure actuelle, la GRC n'utilise pas la reconnaissance faciale sur les photos ou vidéos prises par des SATP.

Le diagramme suivant présente une ventilation des vols effectués par les SATP de la GRC en 2022, par type de mission.

Diagramme 4 : Vols effectués par des SATP de la GRC en 2022, par type de mission



**Autre* comprend la production de vidéos, l'inspection de pylônes radio, le contrôle de la circulation, la cartographie de secteurs pour la planification de la sécurité, l'enregistrement d'images pour les plans d'urgence en cas de tireur actif, et d'autres opérations policières où un SATP de la GRC a été utilisé.

Technologies émergentes

La GRC est résolue à examiner et à déployer les technologies nouvelles et émergentes de façon éthique et responsable. Le PNIT continuera, dans le cadre de son mandat, de publier des informations sur l'utilisation des technologies opérationnelles clés par la GRC, comme l'intelligence artificielle et la reconnaissance faciale, les caméras d'intervention[25], le système de reconnaissance automatique des plaques d'immatriculation[26] et les sources d'information comme les renseignements de sources ouvertes.

Considérations liées aux renseignements de sources ouvertes

Par « renseignements de sources ouvertes », on entend la collecte et l'analyse légales d'informations accessibles au public aux fins d'application de la loi et de prévention du crime. Cela englobe une vaste gamme de sources, y compris les sites Web de nouvelles, les plateformes de médias sociaux, les dossiers publics, les publications universitaires et les autres ressources en ligne auxquelles tout le monde peut accéder librement. La GRC reconnaît que cela peut comprendre des renseignements personnels et qu'il pourrait y avoir une certaine attente en matière de vie privée, même quand ces renseignements sont communiqués publiquement.

La GRC exploite stratégiquement les renseignements de sources ouvertes à diverses fins d'enquêtes et de sécurité publique. Ces applications contribuent au recensement et à la surveillance des menaces, à la localisation de personnes d'intérêt, à la fourniture de soutien aux enquêtes, et à la sensibilisation et à la mobilisation communautaire.

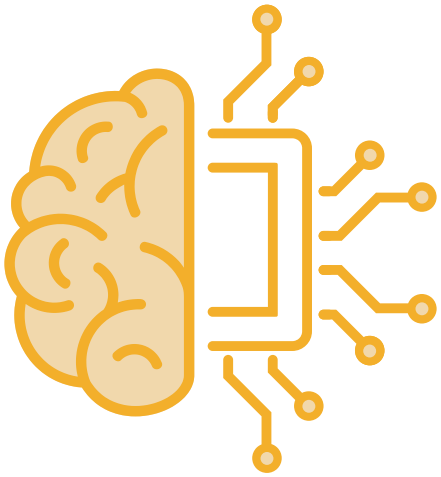
La GRC a recours à divers outils et techniques spécialisés pour analyser les informations de sources ouvertes afin de produire des renseignements de sources ouvertes. Par exemple, un de ces outils est Babel X, pour lequel la GRC a effectué une EFVP détaillée[27].

Ce type de technologie comprend aussi de nombreux outils alimentés par l'intelligence artificielle. Comme le décrit la rubrique suivante, la GRC prend diverses mesures pour s'assurer que l'utilisation de ces outils est légale, éthique, et conforme aux lois canadiennes en matière de protection de la vie privée.

Considérations liées à l'intelligence artificielle

Les organismes d'application de la loi ont de plus en plus recours à l'intelligence artificielle (IA) pour améliorer l'efficacité de différentes fonctions ou tâches, dont la prévision de la criminalité, le classement et l'édition de gros volumes de preuves sur photo et vidéo, la détection de coups de feu, et les services de transcription et de traduction. L'utilisation de l'IA par les organismes d'application de la loi soulève des questions d'ordre éthique liées aux atteintes à la vie privée et aux partis pris potentiels. Il est important de tenir compte de ce qui suit pour veiller à une utilisation éthique et responsable de l'IA.

- Un système d'intelligence artificielle devrait être transparent quant à la façon dont il prend des décisions. Il doit être facile pour les humains de comprendre comment un algorithme d'apprentissage automatique est parvenu à une certaine décision, pour faciliter le dégagement et la correction des erreurs et des partis pris.
- Des mesures de responsabilisation doivent être établies pour s'assurer que les systèmes d'intelligence artificielle fonctionnent comme prévu. Cela exige une surveillance rigoureuse, ainsi qu'une recherche et une évaluation continues.
- Les systèmes d'intelligence artificielle doivent être conçus de façon à éviter les pratiques discriminatoires et les partis pris existants. Un parti pris peut se solder par un résultat injuste pour des groupes marginalisés, et perpétuer les injustices dans le système de justice pénale.
- Les systèmes d'intelligence artificielle sont capables de recueillir et/ou d'analyser de vastes quantités de renseignements personnels, ce qui soulève des questions liées au droit à la vie privée et à l'usage abusif potentiel par les organismes d'application de la loi. Il est important de veiller au respect des droits liés à la vie privée lorsque l'intelligence artificielle est utilisée.



Ces considérations concordent avec les 10 principes clés utilisés par le PNIT pour évaluer les technologies. L'utilisation de l'IA par la GRC doit aussi être conforme aux politiques et directives applicables du gouvernement du Canada.

En outre, le PNIT a récemment corédigé la *Directive provisoire sur les outils d'intelligence artificielle générative de la GRC* pour guider les employés de la GRC en attendant que la politique officielle sur l'IA soit terminée.

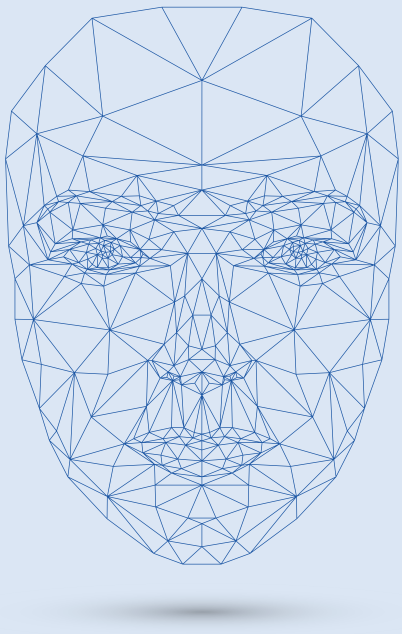
Considérations liées à la reconnaissance faciale

La reconnaissance faciale est une technologie puissante qui a recours à des algorithmes avancés pour traiter des images de visage, et analyser les caractéristiques biométriques faciales à des fins de vérification de l'identité. Son utilisation inappropriée pourrait avoir un impact considérable à le droit à la vie privée et d'autres droits fondamentaux, notamment en raison des risques associés aux biais de données et aux erreurs d'identification.

Dans le contexte de l'application de la loi et de la sécurité publique, la reconnaissance faciale peut contribuer à l'identification de personnes soupçonnées d'avoir commis un crime, de personnes portées disparues ou d'enfants susceptibles d'être victimes d'exploitation sexuelle en ligne, ainsi qu'aux enquêtes connexes, ou aider à atténuer les menaces imminentes à la sécurité publique.

La GRC comprend que l'utilisation de reconnaissance faciale par la police puisse soulever des inquiétudes dans la population canadienne. La GRC utilisera un type de reconnaissance faciale appelée la correspondance faciale, qui est une fonctionnalité intégrée à certaines applications logicielles utilisées pour le traitement, le tri et l'analyse de grands volumes d'images et de vidéos. La GRC utilisera cette technologie exclusivement pour traiter les éléments de preuve qui ont été obtenus légalement dans le cadre d'une enquête.

La GRC prévoit toutefois utiliser des technologies opérationnelles aux fins d'identification faciale à l'avenir, pour aider les enquêteurs à identifier les criminels et les victimes de crimes. Ces types de technologies opérationnelles ne seront utilisées que dans des circonstances précises, conformément aux politiques de la GRC et aux lois canadiennes.



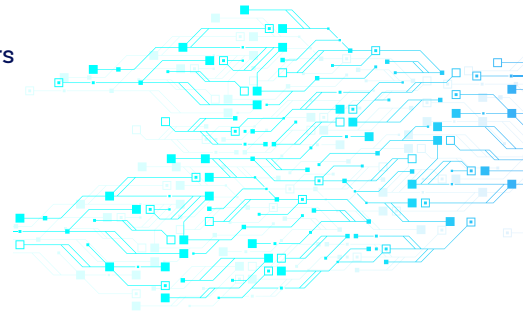
Quelle est la différence entre correspondance faciale et identification faciale?

Reconnaissance faciale : Technologie qui utilise des applications logicielles complexes permettant de détecter et d'analyser des visages apparaissant dans des médias numériques, en vue de comparer les caractéristiques faciales des personnes dont les visages sont détectés et celles apparaissant dans d'autres photos ou vidéos.

Correspondance faciale : Utilisation de la reconnaissance faciale aux fins de comparaison et de regroupement de médias numériques dans lesquels les mêmes visages ou des visages similaires apparaissent. Cette technologie n'est pas utilisée pour identifier directement des individuels inconnus apparaissant dans des photos ou des vidéos. La correspondance faciale peut être obtenue au moyen d'algorithmes moins complexes et d'une puissance de calcul moindre que l'identification faciale. Elle est généralement utilisée pour traiter de grandes quantités d'images ou d'enregistrements vidéo légalement obtenus.

Identification faciale : Utilisation de la reconnaissance faciale aux fins de recherche automatisée d'un visage ou d'une « image de comparaison » d'une personne inconnue dans un fichier local ou une base de données d'images numériques de personnes connues aux fins d'identification ou de vérification. L'identification faciale emploie des algorithmes complexes, l'apprentissage machine, et une importante puissance de calcul pour analyser des caractéristiques faciales, des distances et des motifs afin de parvenir à une identification exacte.

Le PNIT a établi un groupe de travail sur la reconnaissance faciale pour aider à élaborer une politique opérationnelle qui guidera l'utilisation de cette technologie par la GRC. Cette politique reposera sur la consultation d'acteurs du domaine juridique, de la protection de la vie privée et de la société civile et d'autres experts en la matière, pour faire en sorte que la GRC utilise la reconnaissance faciale de façon légale, nécessaire et appropriée.

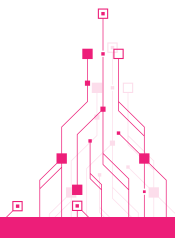


Conclusion

La transparence est essentielle pour inspirer la confiance envers la GRC, et une plus grande transparence concernant les technologies opérationnelles nouvelles et en évolution est déterminante. Le CPVP, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes, et bien d'autres ont clairement énoncé que le Parlement et la population ont le droit de savoir comment ces nouvelles technologies sont utilisées par les organismes d'application de la loi, et comment les répercussions de ces technologies sur la vie privée sont prises en considération.

Le PNIT de la GRC, en collaboration avec d'autres services de police et parties prenantes, prendra d'importantes mesures pour améliorer la responsabilisation grâce à la transparence quant à l'utilisation des technologies opérationnelles par la GRC.

La publication du *Plan de transparence : Aperçu des technologies opérationnelles* est un premier pas important vers une plus grande transparence. Mesurer ces améliorations n'est pas une affaire ponctuelle et ne doit pas être perçu comme se résumant à l'application d'une liste de vérification. Le PNIT continuera d'appuyer les efforts continus de la GRC pour améliorer la transparence et la compréhension du public à l'égard de son utilisation des technologies opérationnelles.



Notes en fin d'ouvrage

1 Pour consulter l'Engagement de transparence en matière de sécurité nationale du gouvernement du Canada : https://www.canada.ca/fr/services/defense/securitenationale/engagement-transparence-securite-nationale.html

2 https://www.tbs-sct.canada.ca/pol/doc-fra.aspx?id=18308

3 Le Programme national d'intégration de la technologie a été créé dans la foulée du rapport de juin 2021 du Commissariat à la protection de la vie privée intitulé *Technologie de reconnaissance faciale : utilisation par les services de police du Canada et approche proposée*. Pour en savoir plus : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/ar_index/202021/sr_grc/

4 https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/rapport-6

5 https://www.noscommunes.ca/documentviewer/fr/44-1/ETHI/rapport-7

6 L'Association internationale des chefs de police a publié un Cadre stratégique de la technologie (2014) afin d'orienter le déploiement responsable et efficace des technologies opérationnelles par les services de police. Le cadre peut être consulté (en anglais seulement) à l'adresse : https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf

7 Pour consulter les résumés des Évaluations des facteurs relatifs à la vie privée de la GRC : https://www.rcmp-grc.gc.ca/fr/addendums-evaluation-des-facteurs-relatifs-la-vie-privee

8 Le recours à l'Analyse comparative entre les sexes Plus (ACS Plus) permet de veiller à ce que les politiques, les programmes et les processus de la GRC soient inclusifs et favorisent un environnement de travail sain et sécuritaire. Pour en savoir plus sur les efforts déployés par la GRC au chapitre de l'ACS Plus : https://www.rcmp-grc.gc.ca/fr/changement-a-grc/soutenir-police-moderne/accroitre-lutilisation-lanalyse-genre-acs-lensemble-grc

9 Pour en savoir plus sur le projet de mise en service des caméras d'intervention de la GRC : https://rcmp.ca/fr/projet-cameras-dintervention

10 Pour en savoir plus sur le programme de technologie de reconnaissance automatique des plaques d'immatriculation en Colombie-Britannique : https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?languageId=4&siteNodeId=23&contentId=11953

11 En novembre 2022, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique a présenté à la Chambre des communes un rapport intitulé *Outils d'enquête sur appareil utilisés par la Gendarmerie royale du Canada et enjeux liés*. Pour consulter le rapport : https://www.noscommunes.ca/DocumentViewer/fr/44-1/ETHI/rapport-7

12 Bellovin, Steven M., Matt Blaze, Sandy Clark et Susan Landau. « Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet », *Nw. J. Tech. & Intell. Prop.*, vol. 12, n° 1 (2014). Sur Internet : https://scholarlycommons.law.northwestern.edu/njtip/vol12/iss1/1[en anglais seulement]

13 En vertu de la partie *VI du Code criminel*, le ministre de la Sécurité publique et de la Protection civile doit préparer et présenter au Parlement un rapport annuel sur le recours à la surveillance électronique pour les infractions qui peuvent faire l'objet de poursuites par le procureur général du Canada ou en son nom. Cette exigence vise la GRC et le milieu plus large d'application de la loi au Canada. Pour consulter le *Rapport annuel sur la surveillance électronique 2020,* qui couvre une période de cinq allant de 2016 à 2020 : https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2022-nnl-rprt-lctrnc-srvllnc/index-fr.aspx

14 Pour consulter le Rapport d'incident de la GRC - 2021 : https://www.rcmp-grc.gc.ca/transparenc/police-info-policieres/calls-appels/occurence-incident/2021/index-fra.htm

15 Un incident désigne tout type d'événement ou d'activité nécessitant l'intervention de la police et qui est consigné dans un système de gestion des dossiers de la police.

16 L'article 183 du *Code criminel* fournit la liste complète des infractions criminelles qui pourraient se prêter à l'utilisation d'outils d'enquête embarqués par la GRC. https://www.laws-lois.justice.gc.ca/fra/lois/c-46/section-183.html

17 Lorsque l'urgence de la situation l'exige, la GRC peut utiliser des outils d'enquête embarqués sans obtenir d'autorisation judiciaire préalable, notamment dans les cas d'enlèvement, lorsqu'une victime est exposée à un danger immédiat, et que l'urgence de la situation rend difficilement réalisable l'obtention du mandat. L'article 529.3 du *Code criminel* comprend une définition de « situation d'urgence » applicable à l'entrée dans une maison d'habitation sans mandat, qui s'ajoute à la jurisprudence canadienne. Bien que ce scénario soit possible, à ce jour, la GRC n'a jamais déployé d'outil d'enquête embarqué sans avoir obtenu une autorisation judiciaire préalable.

18 Les identifiants uniques comprennent les numéros d'identité internationale d'abonnement mobile et d'équipement mobile associés aux appareils mobiles (cellulaires).

19 En 2017, le Commissariat à la protection de la vie privée du Canada a enquêté sur l'utilisation par la GRC des simulateurs de station cellulaire, en vertu de la *Loi sur la protection des renseignements personnels*. Pour consulter un résumé de l'enquête et des constatations : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-institutions-federales/2016-17/pa_20170816_rcmp

20 Lorsque l'urgence de la situation l'exige, la GRC peut utiliser des simulateurs de site cellulaire sans obtenir d'autorisation judiciaire préalable, notamment dans les cas d'enlèvement, lorsqu'une victime est exposée à un danger immédiat, et que l'urgence de la situation rend difficilement réalisable l'obtention du mandat. L'article 529.3 du *Code criminel* comprend une définition de « situation d'urgence » applicable à l'entrée dans une maison d'habitation sans mandat, qui s'ajoute à la jurisprudence canadienne.

21 Innovation, Sciences et Développement économique Canada est responsable de la gestion et de la réglementation du spectre des radiofréquences au Canada.

22 Le Programme des systèmes d'aéronef télépiloté de la GRC n'utilise pas la technologie de la reconnaissance faciale comme capacité technique pour la surveillance aérienne.

23 Les membres des groupes tactiques d'intervention de la GRC ont recours à des tactiques, à des armes et à de l'équipement spécialisés pour mettre fin à des situations à haut risque. Pour en savoir plus sur le Groupe tactique d'intervention de la GRC : https://www.rcmp-grc.gc.ca/ert-gti/index-fra.htm

24 Pour consulter le résumé du Programme des systèmes d'aéronef télépiloté (SATP) : https://www.rcmp-grc.gc.ca/fr/programme-des-systemes-daeronef-telepilote-satp-resume

25 Pour en savoir plus sur le projet de mise en service des caméras d'intervention de la GRC : https://rcmp.ca/fr/projet-cameras-dintervention

26 Pour en savoir plus sur le programme de technologie de reconnaissance automatique des plaques d'immatriculation en Colombie-Britannique : https://bc-cb.rcmp-grc.gc.ca/ViewPage.action?languageId=4&siteNodeId=23&contentId=11953

27 https://www.rcmp-grc.gc.ca/fr/plateforme-babel-x

No de cat. PS64-231/2024F-PDF
ISBN 978-0-660-72510-9