Commissariat
à la protection de la
vie privée du Canada

VÉRIFICATION DE CERTAINES BASES DE DONNÉES OPÉRATIONNELLES DE LA GRC

Rapport de vérification de la commissaire à la protection de la vie privée du Canada

Article 37 de la *Loi sur la protection des renseignements personnels*

RAPPORT FINAL

2011

Commissariat à la protection de la vie privée du Canada
112, rue Kent
Ottawa, Ontario
K1A 1H3

(613) 947-1698, 1-800-282-1376
Téléc. : (613) 947-6850
ATS : (613) 992-9190
Suivez nous sur Twitter : @privacyprivee

Nº de catalogue IP54-42/2011
ISBN 978-1-100-53857-0

Cette publication est également disponible sur notre site Web à **www.priv.gc.ca**.

Table des matières

Principaux éléments

POINTS EXAMINÉS

Les responsables de l'application de la loi et de la justice pénale du Canada disposent d'un imposant réseau de systèmes de bases de données pour les aider à appliquer les lois, à prévenir les crimes, à mener des enquêtes et à maintenir la paix, l'ordre et la sécurité. En tant que service de police national du pays, la Gendarmerie royale du Canada (GRC) a dirigé les efforts visant à cerner les besoins, à élaborer des systèmes d'information et des services connexes et à les rendre accessibles à l'ensemble du milieu policier.

Notre vérification était axée sur deux de ces systèmes choisis en raison de leur importance et de leur utilisation intensive par la GRC et d'autres organismes responsables de l'application de la loi : le Centre d'information de la police canadienne (CIPC) et le Système d'incidents et de rapports de police (SIRP). Le CIPC offre un service informatisé de stockage et de recherche d'informations sur les crimes et les criminels. Le SIRP est le principal système de gestion des dossiers opérationnels de la GRC.

La vérification a porté sur les politiques et procédures de la GRC régissant l'accès au CIPC et son utilisation, sur les politiques et procédures relatives à la suppression des renseignements personnels du SIRP devenus superflus, sur les pratiques de la GRC concernant l'examen de la conformité aux modalités d'utilisation du CIPC et du SIRP et sur la gestion des droits d'accès accordés aux utilisateurs du SIRP.

IMPORTANCE DE CET ENJEU

Le CIPC et le SIRP contiennent tous deux une grande quantité de renseignements personnels sensibles qui, s'ils étaient utilisés ou communiqués de façon inappropriée, pourraient avoir une incidence considérable sur les droits et libertés des personnes touchées ainsi que sur leur réputation, leur employabilité et leur sécurité. Une atteinte à la sécurité pourrait aussi mettre en péril des enquêtes policières en cours. Chaque année, la GRC produit un rapport sur les atteintes à la sécurité liées au CIPC. Bon nombre d'entre elles sont causées par la consultation non autorisée et l'utilisation inappropriée de renseignements personnels qui peuvent avoir des répercussions considérables sur la vie privée des personnes affectées.

La GRC a également constaté que certains services de police diffusaient des détails sur des condamnations, des remises en liberté ou des réhabilitations à des employeurs sans le consentement éclairé des employés éventuels, contrevenant ainsi à la politique du CIPC.

L'information qui se trouve dans ces bases de données est accessible à une vaste gamme de responsables de l'application de la loi, qu'ils soient au bureau ou sur la route, par exemple :

- les banques de données du CIPC comprennent des renseignements sur des permis de conduire et des plaques d'immatriculation, des véhicules et des bateaux volés, des mandats d'arrêt, des personnes et des biens disparus, des casiers

judiciaires, des empreintes digitales, des armes à feu enregistrées et des enfants disparus. Le CIPC contient plus de dix millions de documents, et plus de 200 millions de demandes ont été traitées à partir de 40 000 points d'accès en 2009;

- le SIRP est un système global de gestion des incidents et des dossiers comprenant de l'information sur les gens qui ont été en contact avec la police en tant que suspects, victimes, témoins ou contrevenants, depuis le signalement de l'incident jusqu'à la conclusion définitive. La GRC et 23 services de police partenaires utilisent le SIRP comme système de gestion des dossiers opérationnels. Environ 1,6 million de dossiers d'incidents sont traités chaque année.

La GRC est responsable du stockage et de la récupération des renseignements judiciaires partagés ainsi que de leur communication à tous les organismes agréés de justice pénale et aux autres organismes travaillant à la détection et à la prévention du crime ainsi qu'aux enquêtes. Elle est dans l'obligation de protéger la vie privée des personnes, et donc les renseignements personnels dont elle a la charge.

CONSTATATIONS

Centre d'information de la police canadienne

La GRC a élaboré et mis en œuvre des politiques et des procédures pour protéger les renseignements personnels des Canadiennes et Canadiens qui sont consultés et utilisés dans la base de données du CIPC. Des atteintes à la protection des renseignements personnels ont eu lieu, mais relativement rarement. En outre, des mécanismes sont en place pour enquêter sur ces atteintes et prendre des mesures à la suite des enquêtes. Bon nombre de ces atteintes découlaient de requêtes effectuées dans le CIPC à des fins personnelles. Les enquêtes montrant que le CIPC a été mal utilisé peuvent entraîner la modification de la politique du CIPC, une réprimande, une suspension ou un licenciement.

La GRC a établi des protocoles d'entente (PE) pour régir l'utilisation du CIPC par les organismes dont les pouvoirs d'application de la loi sont limités ou qui jouent des rôles complémentaires dans le cadre de l'application de la loi. Toutefois, la GRC n'a pas encore conclu de PE officiel avec environ 25 % des services de police ayant accès au CIPC.

Des vérifications sont régulièrement effectuées pour examiner les enquêtes de sécurité sur le personnel et la sécurité sur le terminal et sur le site à interface du CIPC, ainsi que pour veiller à ce que tous les organismes, la GRC comprise, respectent la politique et les lignes directrices du Manuel de référence du CIPC. Ce système de surveillance vise à faire en sorte que tous les utilisateurs se conforment aux exigences énoncées dans la politique du CIPC, y compris aux principes de protection de la vie privée.

La GRC a appris que des incidents sont survenus récemment : des services de police diffusaient des renseignements sur les antécédents judiciaires tirés du système du CIPC, ce qui contrevient directement à la politique du CIPC, à la *Loi sur le casier judiciaire*, à la *Loi sur le système de justice pénale pour les adolescents* et à la Directive ministérielle sur la divulgation de renseignements sur les antécédents judiciaires. Un certain nombre de services diffusaient des détails sur des condamnations, des remises en liberté ou des réhabilitations aux employeurs sans le consentement éclairé de l'employé éventuel et sans confirmer l'identité de la personne concernée en comparant les empreintes digitales. En novembre 2009, la GRC a réagi à ces communications en diffusant une directive à l'intention des utilisateurs du CIPC pour les aviser que certains organismes ne respectaient pas les politiques et les procédures établies relatives à l'utilisation du système. Cette mesure a été renforcée en août 2010 lorsque le ministre de la Sécurité publique a émis une directive afin de clarifier dans quelles conditions les renseignements sur les casiers judiciaires qui se trouvent dans le CIPC pouvaient être utilisés et communiqués.

Système d'incidents et de rapports de police

La GRC a élaboré un ensemble complet de politiques, de procédures de fonctionnement normalisées et d'ententes pour garantir que le SIRP soit utilisé en conformité avec les principes énoncés dans la *Loi sur la protection des renseignements personnels*. Cependant, la suppression de certains renseignements, une meilleure gestion des droits d'accès, des examens systématiques et un accès plus efficace aux journaux sur les activités des utilisateurs sont nécessaires pour que les utilisateurs du SIRP respectent les politiques et les procédures de la GRC ainsi que les lois provinciales et fédérales en matière de protection de la vie privée.

La GRC a élaboré des politiques et des procédures d'exploitation normalisées qui indiquent pendant combien de temps les renseignements personnels peuvent être conservés dans le SIRP avant d'être isolés ou supprimés. Cependant, les renseignements personnels sont conservés plus longtemps, contrairement aux dispositions de la *Loi sur la protection des renseignements personnels*. En outre, la GRC ne dispose d'aucun processus pour supprimer l'accès aux dossiers sur les condamnations ayant fait l'objet d'une réhabilitation ou sur les condamnations injustifiées.

Aucun examen actif des comptes d'utilisateur du SIRP n'est effectué. La politique de la GRC sur le SIRP stipule que le droit d'accès d'un utilisateur doit être révoqué si celui ci n'en a plus besoin pour exécuter ses tâches professionnelles ou après 14 mois d'inactivité, mais nous avons vu que plus de 1 000 utilisateurs ayant un compte actif n'avaient pas consulté le SIRP depuis 14 mois ou plus. Nous avons aussi constaté que le processus d'examen de l'activité des utilisateurs du SIRP est lourd, ce qui complique les enquêtes sur les utilisations indues du système.

La GRC n'a pas été en mesure de démontrer qu'elle examine systématiquement les utilisateurs du SIRP pour s'assurer que les renseignements personnels sont utilisés en conformité avec les politiques en vigueur.

La GRC a répondu à nos constatations; ses réponses sont indiquées après nos recommandations tout au long du présent rapport.

Introduction

CONTEXTE

1. La GRC est le service de police national du Canada. Elle compte environ 30 000 membres et employés dont le mandat consiste notamment à prévenir les crimes, à mener des enquêtes, à maintenir la paix et l'ordre, à appliquer les lois, à contribuer à la sécurité nationale et à protéger les hommes d'État, les dignitaires en visite et les missions étrangères.

2. La GRC applique les lois fédérales partout au pays ainsi que les lois provinciales et territoriales dans l'ensemble des provinces et territoires (exception faite du Québec et de l'Ontario). Elle offre aussi des services de police à forfait à près de 200 municipalités. La GRC fournit également des services d'enquête et de soutien opérationnel à plus de 500 organismes canadiens d'application de la loi et de justice pénale.

3. Le CIPC et le SIRP sont deux des bases de données à la disposition de la GRC pour assurer ces services.

4. Le CIPC offre un service informatisé de stockage et de recherche d'informations sur les crimes et les criminels. Il est très utilisé dans le milieu de l'application de la loi et de la justice pénale. En 2009, le CIPC possédait 10 millions de documents et a traité plus de 200 millions de requêtes à partir de 40 000 points d'accès. Il permet à plus de 80 000 agents de la paix de se connecter au système informatique central dans plus de 3 000 services de police, détachements de la GRC et organismes fédéraux et provinciaux de l'ensemble du pays.

5. Les banques de données du CIPC comprennent des renseignements sur des permis de conduire et des plaques d'immatriculation, des véhicules et des bateaux volés, des mandats d'arrêt, des personnes et des biens disparus, des casiers judiciaires, des empreintes digitales, l'enregistrement d'armes à feu, des enfants disparus, etc. Le CIPC est considéré comme le pilier du système de justice pénale. Il permet aux responsables de l'application de la loi d'avoir accès à une grande quantité d'informations sur les Canadiennes et Canadiens. Les tribunaux, les commissions des libérations conditionnelles et les ministères et organismes gouvernementaux comme le Service correctionnel du Canada et l'Agence des services frontaliers du Canada ont aussi recours au CIPC dans divers buts.

6. Le SIRP est le système de gestion des relevés judiciaires de la GRC. Il s'agit d'un système de gestion des dossiers comprenant des renseignements sur les gens qui ont été en contact avec la police en tant que suspects, victimes, témoins ou contrevenants. Le SIRP a été instauré en 2003 dans le but de conserver la trace de tous les aspects d'une enquête depuis le signalement de l'incident jusqu'à la conclusion définitive si l'affaire est portée devant les tribunaux. La GRC utilise le SIRP comme système de gestion des dossiers opérationnels, tout comme 23 services de police partenaires de petite taille (comptant généralement moins de 300 agents) qui ne possèdent pas leur propre système électronique de gestion des dossiers.

ENCADRÉ Nº 1 : EXEMPLE D'UTILISATION DU CIPC ET DU SIRP

Un agent de la GRC arrête un conducteur pour excès de vitesse. Il commence par entrer une requête dans le CIPC pour voir si le véhicule a été volé ou si le conducteur est visé par un mandat non exécuté. L'agent peut ensuite faire une recherche dans le SIRP pour savoir si le véhicule ou le conducteur ont été impliqués dans d'autres incidents. Un dossier d'incident est créé dans le SIRP pour prendre note de l'événement. Le dossier sera mis à jour pour rendre compte des faits ultérieurs, par exemple des accusations portées et des décisions prises à leur sujet.

THÈME DE LA VÉRIFICATION

7. La vérification visait à déterminer si la GRC gère adéquatement les renseignements personnels contenus dans les bases de données du CIPC et du SIRP.

8. Nous n'avons pas examiné comment les renseignements contenus dans ces bases de données influaient sur les décisions prises dans le cadre des activités quotidiennes de la GRC. De plus, la vérification n'a pas porté sur les mesures de sécurité prises par d'autres utilisateurs du CIPC et du SIRP que la GRC. L'information contenue dans le CIPC est diffusée à l'échelle internationale par l'entremise d'Interpol et est communiquée aux organismes américains d'application de la loi comme l'United States Customs and Border Protection (USCBP). La vérification n'a pas porté sur les mesures de sécurité liées à ces ententes d'échange de renseignements.

9. La section **À propos de la vérification** du présent rapport donne plus de détails sur l'objectif, la portée, la démarche et les critères de la vérification.

Observations et recommandations

CENTRE D'INFORMATION DE LA POLICE CANADIENNE (CIPC)

10. Le commissaire de la GRC est l'instance de gouvernance de l'ensemble du CIPC. Le Comité consultatif du CIPC formule des conseils et des recommandations au commissaire pour ce qui est d'établir le champ d'application du CIPC et de déterminer l'admissibilité des organismes participants. Le Comité consultatif du CIPC est composé de représentants des grands services de police et d'organismes fédéraux et provinciaux d'application de la loi.

11. La GRC est chargée d'héberger la base de données du CIPC, d'établir des contrôles et de veiller à ce que des activités de surveillance soient menées. En fonction du mandat de l'organisme qui consulte la base de données du CIPC, la GRC accordera un niveau d'accès approprié en se basant sur une recommandation du Comité consultatif du CIPC. Afin de garantir le respect des modalités suivant lesquelles l'accès a été accordé, la GRC supervise un programme de vérification pour que des examens soient effectués régulièrement. Ces vérifications permettent notamment d'examiner si les données qui doivent être entrées dans la base de données du CIPC sont complètes et si l'accès au système est suffisamment sécurisé. Cependant, la responsabilité de fournir des renseignements exacts en temps opportun incombe uniquement à l'organisme qui entre les données dans le CIPC.

12. Compte tenu de la sensibilité des renseignements personnels qui se trouvent dans cette base de données, nous espérions que des politiques et des procédures soient en place pour que les utilisateurs du CIPC bénéficient d'un niveau d'accès adapté. Nous nous attendions également à ce que la GRC ait établi des règles concernant l'accès à cette base de données et l'utilisation appropriée de celle ci et vérifie si les utilisateurs les respectent pour éviter la communication non autorisée de renseignements personnels.

13. Nous avons examiné si la GRC :

    - dispose de politiques et de procédures pour régir l'accès aux renseignements personnels contenus dans le CIPC et leur utilisation;
    - surveille le respect par les utilisateurs des modalités d'accès et d'utilisation relatives au CIPC.

Les politiques et les procédures destinées à protéger les renseignements personnels consultés à partir du CIPC sont bien établies

14. Le Comité consultatif du CIPC examine les demandes d'accès au système des organismes et, s'il donne son approbation, les transfère à la GRC pour qu'elles soient traitées. Un certain nombre de niveaux d'accès peuvent être accordés en fonction du mandat de l'organisme demandeur.

15. La politique stipule que, si l'accès au CIPC est accordé à un organisme, la GRC doit réaliser une évaluation de sécurité pour s'assurer que l'infrastructure technique de l'organisme est appropriée. Nous avons examiné le processus d'évaluation et constaté que les exigences comportent de nombreux éléments essentiels pour sécuriser l'environnement, dont la sécurité physique, l'authentification des utilisateurs et les paramètres de configuration nécessaires pour sécuriser le réseau. Nous considérons que le

cadre d'évaluation de la sécurité est suffisamment solide et complet, mais la GRC n'a pu démontrer que tous les organismes ayant accès au CIPC avaient fait l'objet d'une évaluation de sécurité.

16. Des politiques, des procédures et des ententes écrites ont été mises en place pour protéger les renseignements personnels en raison de la grande quantité de données enregistrées dans le CIPC et du nombre important d'utilisateurs. Des PE comprenant des clauses sur la protection de la vie privée établissent les modalités liées à l'utilisation du CIPC par les organismes membres. La GRC a réuni les politiques et les procédures dans un même document : le *Manuel de référence du CIPC* (le Manuel).

17. Le Manuel comprend les politiques et les procédures utilisées pour réglementer les opérations générales du CIPC et il aborde les principes relatifs à l'équité dans le traitement de l'information énoncés dans la *Loi sur la protection des renseignements personnels*. On y trouve des principes sur l'utilisation, la collecte, l'exactitude, la protection, la conservation et l'élimination des données.

18. La GRC a appris que des incidents sont survenus récemment : des services de police diffusaient des renseignements sur les antécédents judiciaires tirés du système du CIPC, ce qui contrevient directement à la politique du CIPC, à la *Loi sur le casier judiciaire*, à la *Loi sur le système de justice pénale pour les adolescents* et à la Directive ministérielle sur la divulgation de renseignements sur les antécédents judiciaires. La GRC nous a informés qu'un certain nombre de services diffusaient des détails sur les condamnations, les remises en liberté ou les réhabilitations aux employeurs sans le consentement éclairé de l'employé éventuel et sans confirmer l'identité de la personne concernée en comparant les empreintes digitales.

19. En novembre 2009, la GRC a réagi à ces communications en diffusant une directive à l'intention des utilisateurs du CIPC pour les aviser que certains organismes ne respectaient pas les politiques et les procédures en vigueur relativement à l'utilisation du système du CIPC. Puis, en août 2010, le ministre de la Sécurité publique a émis une directive afin de clarifier dans quelles conditions les renseignements sur les casiers judiciaires qui se trouvent dans le CIPC peuvent être utilisés et communiqués.

20. Une entente écrite, par exemple un PE, régit la conformité avec la politique du CIPC. Des PE entre la GRC et les organismes membres sont en place pour réglementer l'accès au CIPC. Ils varient quelque peu en fonction de la catégorie de l'organisme ou, dans certains cas, de son mandat précis, mais tous les PE comprennent des procédures à respecter en ce qui a trait au traitement des renseignements personnels contenus dans la base de données. Des exigences relatives aux cotes de sécurité du personnel ayant accès au CIPC, dont la vérification des casiers judiciaires et la formation obligatoire, sont établies. Les PE précisent la marche à suivre lorsque l'on diffuse des renseignements du CIPC et obligent les organismes à signaler tout incident connu ou soupçonné. Ils stipulent que les organismes doivent se conformer aux lois provinciales et fédérales applicables en matière d'accès à l'information et de protection des renseignements personnels. Un organisme qui ne respecte pas ses obligations risque de perdre ses privilèges d'accès au CIPC.

21. La GRC a conclu des PE avec des organismes dont les pouvoirs d'application de la loi sont limités, comme l'Agence des services frontaliers du Canada, l'Agence du revenu du Canada, Citoyenneté et Immigration Canada, le Service correctionnel du Canada et la Commission nationale des libérations conditionnelles. Des organismes jouant un rôle complémentaire en matière d'application de la loi, comme Passeport Canada, Transports Canada et le Bureau d'assurance du Canada, disposent aussi d'un PE. Les PE en vigueur sont renouvelés périodiquement. À ce moment, les exigences imposées aux organismes relativement à l'accès sont réévaluées et maintenues ou modifiées.

22. Par contre, la GRC n'a pas encore établi de PE officiel avec environ 25 % des services de police qui ont accès au CIPC. Auparavant, il n'était pas nécessaire d'établir un PE avec ces services, car l'accès au CIPC leur était accordé parce que leur rôle de base est de maintenir l'ordre. Pendant notre vérification, la GRC négociait les modalités d'utilisation avec les services de police qui n'avaient pas encore de PE.

23. RECOMMANDATION

Le CIPC devrait établir un échéancier clair concernant l'établissement de PE, comprenant des clauses sur la protection des renseignements personnels, avec tous les services de police.

Réponse de la GRC :

Comme l'a demandé le sous-commissaire, Soutien aux services de police, en novembre 2010, le CIPC négocie activement avec les derniers services de police (25 %) qui n'ont pas encore signé de PE. Comme prévu, le modèle de PE ne s'applique pas nécessairement dans tous les cas et les différences font l'objet de discussions pour que des PE soient conclus d'ici le 31 mars 2012.

24. Selon la politique du CIPC, les utilisateurs d'un organisme approuvé doivent recevoir une formation appropriée avant d'avoir accès au CIPC. Le programme de formation comprend des modules montrant aux utilisateurs quelles sont leurs obligations en matière de protection des renseignements personnels et les utilisations acceptables du CIPC. Les utilisateurs sont également avisés que le CIPC doit être utilisé pour des motifs légitimes et non à des fins personnelles, et que les pratiques contraires à la politique du CIPC feront l'objet d'une enquête pouvant entraîner des pénalités ou des conséquences allant de la formation de consolidation au licenciement en passant par une amende ou une suspension.

25. Nous avons examiné les mesures de contrôle qui sont en place pour veiller à ce que les utilisateurs soient autorisés à accéder au CIPC. Nous avons constaté qu'une stratégie permanente d'atténuation des risques liés à la TI oblige les organismes membres à prendre des mesures de sécurité accrue en exigeant que les utilisateurs aient besoin tant d'un jeton physique que d'un mot de passe pour se connecter au système du CIPC. On parle alors d'une identification et d'une authentification robustes.

26. Nous avons cependant constaté que 33 % des organismes membres du CIPC n'avaient pas encore établi cette procédure d'authentification des utilisateurs en raison des contraintes techniques de leurs infrastructures. L'objectif de la GRC était que ces organismes déploient les mesures de sécurité requises au plus tard en avril 2009. La GRC surveille les progrès des organismes qui accusent un retard à ce sujet.

Un système de surveillance est en place pour régir l'utilisation appropriée

27. Les services de police et d'autres organismes utilisent les renseignements consignés dans le CIPC aux fins d'enquête et d'application de la loi, ce qui a chaque jour des répercussions sur des milliers de Canadiennes et Canadiens. Par conséquent, il est important que les normes et les pratiques du CIPC soient respectées afin de garantir que les renseignements contenus dans le système soient exacts et que les procédures de traitement de l'information soient conformes aux lois applicables dans le domaine de la protection des renseignements personnels.

28. La responsabilité de maintenir les renseignements exacts et à jour incombe à l'organisme du CIPC qui fournit l'information. La GRC envoie chaque mois un rapport de validation à chaque

organisme collaborateur pour examiner l'intégrité des données. Les organismes doivent vérifier la validité et l'exactitude des renseignements qu'ils ont versés dans le système et apporter les modifications nécessaires.

29. La GRC effectue des vérifications des organismes membres du CIPC (sauf au Québec et en Ontario, où les vérifications sont réalisées par la Sûreté du Québec et le ministère de la Sécurité communautaire et des Services correctionnels, respectivement) pour garantir le respect du processus de validation et déterminer si un organisme se conforme aux principes de protection des renseignements personnels énoncés dans la politique du CIPC. Des procédures, des outils et des rapports normalisés sont utilisés. La politique du CIPC exige qu'une vérification de la conformité de chaque organisme avec la politique et les procédures soit réalisée au moins une fois tous les quatre ans. Tout nouvel organisme fait l'objet d'une vérification moins d'un an après avoir obtenu l'accès au CIPC. Au cours de l'exercice financier 2009 2010, 477 vérifications du CIPC ont été réalisées.

30. Les vérificateurs se penchent sur la qualité et l'intégrité des dossiers enregistrés dans le système du CIPC et évaluent le savoir et la compétence du personnel de l'organisme concernant le système. En outre, ils examinent le filtrage de sécurité du personnel et la sécurité sur le terminal et le site à interface du CIPC en plus de s'assurer que tous les organismes respectent la politique et les lignes directrices du Manuel de référence du CIPC.

31. Lorsqu'ils ont terminé leur travail, les vérificateurs préparent un rapport récapitulatif résumant leurs constatations et le distribuent au Comité consultatif du CIPC. Un rapport sur le nombre de vérifications effectuées dans chaque région est publié dans le rapport annuel du CIPC. Une vérification de suivi est réalisée quelques mois après la première vérification pour veiller à ce que les lacunes soient corrigées.

32. Nous avons également observé que la GRC fait le suivi des atteintes à la sécurité des données du CIPC. Elle supervise les enquêtes sur ces atteintes signalées par des services de police et des particuliers. Les atteintes à la sécurité des données sont rares et elles font l'objet d'une enquête. Les activités de vérification ont permis de détecter environ 10 % des incidents liés au CIPC; les autres ont été décelés au moyen d'examens continus ou de plaintes. Plus de 200 millions de requêtes sont faites chaque année dans le CIPC. En 2009, 280 atteintes ont été signalées; 24 étaient fondées, 86 ne l'étaient pas et 170 font toujours l'objet d'une enquête. Bon nombre de ces atteintes consistaient en une requête exécutée à des fins personnelles. Les atteintes à la sécurité peuvent entraîner une modification de la politique du CIPC, une réprimande, une amende, une suspension ou le licenciement de l'employé coupable.

SYSTÈME D'INCIDENTS ET DE RAPPORTS DE POLICE (SIRP)

33. Le SIRP est une base de données de relevés judiciaires utilisée par la GRC et 23 services policiers partenaires comme système de gestion des dossiers opérationnels. Les partenaires sont des services de police de petite taille (comptant moins de 300 agents) qui ne possèdent pas leur propre système électronique de gestion des dossiers. La GRC donne accès aux bases de données du SIRP et héberge les données. Environ 1,6 million de dossiers d'incidents sont traités chaque année à l'aide du SIRP.

34. Le SIRP a été lancé à l'automne 2003 et mis en service partout au pays à l'été 2005. Il sert à conserver la trace de tous les aspects d'une enquête depuis le signalement d'un'incident jusqu'à la conclusion définitive si l'affaire est portée devant les tribunaux. Il comprend de l'information sur les gens qui ont été en contact avec la police en tant que suspects, victimes, témoins ou contrevenants.

35. Compte tenu de la sensibilité des renseignements personnels qui se trouvent dans cette base de données, nous nous attendions à ce que des politiques et des procédures garantissent que les renseignements personnels du SIRP sont traités en conformité avec les exigences prévues par la loi en matière de conservation et d'élimination et soient protégés contre les accès non autorisés. Les politiques et les procédures sur la conservation découlent des lois en vigueur comme la *Loi sur le casier judiciaire* et la *Loi sur le système de justice pénale pour les adolescents*.

36. Nous avons vérifié si la GRC :

- avait établi des politiques et des procédures destinées à supprimer les renseignements personnels du SIRP qui n'étaient plus nécessaires;
- gérait adéquatement l'accès au SIRP;
- surveillait l'utilisation du SIRP pour garantir la conformité avec ses politiques et ses procédures destinées à protéger les renseignements personnels.

Des renseignements personnels sont conservés plus longtemps que nécessaire

37. Nous avons constaté que la GRC a élaboré des politiques et des procédures de fonctionnement normalisées relatives au SIRP qui indiquent combien de temps les renseignements peuvent être conservés avant d'être isolés ou supprimés en vertu des lois en vigueur.

38. La loi prescrit l'isolement de certains renseignements lorsque la période de conservation est terminée, c'est-à-dire que les renseignements doivent être placés dans un répertoire spécial auquel l'accès est très restreint. Les types de renseignements isolés comprennent les détails liés aux libérations inconditionnelles et conditionnelles et aux réhabilitations.

39. La loi exige que tous les documents créés dans le SIRP soient éliminés à la fin de la période de conservation de chaque catégorie de renseignements. Avant la suppression, les dossiers sont évalués pour voir s'ils devraient être conservés par Bibliothèque et Archives Canada.

40. Nous avons examiné les procédures régissant la conservation des renseignements personnels dans le SIRP et constaté que la base de données est conçue pour supprimer tous les renseignements sur les incidents qui ont atteint la date de leur élimination, sauf s'ils ont une valeur archivistique. La GRC a désactivé cette fonction. Par conséquent, les renseignements personnels d'une personne dont les données auraient dû être supprimées sont encore facilement accessibles dans la base de données du SIRP.

41. La GRC a mentionné que cette mesure a été prise pour tirer des renseignements statistiques du SIRP. Par conséquent, les renseignements qui devraient être supprimés parce que la période de conservation est terminée demeurent dans la base.

42. RECOMMANDATION

La GRC devrait éliminer les données du SIRP qui doivent l'être de façon à respecter la *Loi sur la protection des renseignements personnels*.

Réponse de la GRC :

La GRC est d'accord et prendra immédiatement des mesures pour corriger la situation.

43. **Le droit d'accès aux dossiers sur les condamnations ayant fait l'objet d'une réhabilitation n'est pas retiré suivant les besoins.** Durant l'examen des procédures de suppression imposées par la *Loi sur le casier judiciaire* et la *Loi sur le système de justice pénale pour les adolescents*, nous avons constaté que la GRC n'a pas encore enclenché un processus pour supprimer, dans les bases de données du SIRP, les dossiers liés aux condamnations ayant fait l'objet d'une réhabilitation.

44. Ces dossiers ne devraient plus être accessibles à partir du SIRP. Or, si l'on cherche le nom d'une personne réhabilitée dans le système, les détails sur sa condamnation peuvent apparaître.

45. Il est important pour les Canadiennes et Canadiens réhabilités que de tels renseignements ne soient pas communiqués de façon inopportune, car cela pourrait nuire à leurs chances d'obtenir un emploi, de voyager, d'étudier ou de faire du bénévolat. La *Loi canadienne sur les droits de la personne* interdit la discrimination fondée sur un dossier ayant fait l'objet d'une réhabilitation.

ENCADRÉ Nº 2 : COMMUNICATION DE RENSEIGNEMENTS SUR LES INFRACTIONS AYANT FAIT L'OBJET D'UNE RÉHABILITATION OU D'UNE ABSOLUTION

Dans certains cas exceptionnels prévus par la *Loi sur le casier judiciaire*, l'existence d'une infraction ayant fait l'objet d'une réhabilitation ou d'une absolution peut être communiquée. Les nom, date de naissance et domicile de la personne qui a commis une infraction ayant fait l'objet d'une réhabilitation ou d'une absolution peuvent être communiqués à la police pour favoriser l'enquête lorsque les empreintes digitales de cette personne se trouvent sur les lieux d'un crime. Ces renseignements peuvent aussi être divulgués aux services de police compétents pour identifier une personne morte ou amnésique. L'existence d'une condamnation pour une infraction à caractère sexuel peut être communiquée dans le contexte d'une vérification de l'aptitude à travailler auprès de personnes vulnérables. Le représentant autorisé d'un organisme responsable du bien-être de personnes vulnérables peut demander une telle recherche pour faire une vérification sur un demandeur ayant l'intention de travailler ou de faire du bénévolat si celui-ci a donné son consentement écrit à la vérification et à la communication de ces renseignements.

46. **Il n'y a aucune procédure pour supprimer les condamnations injustifiées.** La GRC n'a géré aucun cas connu de condamnation injustifiée depuis la mise en production complète du SIRP en 2005, mais aucune procédure n'est prévue pour supprimer les dossiers liés à de telles condamnations. Il y a des procédures de fonctionnement normalisées pour isoler les renseignements autres que les réhabilitations et traiter les absolutions conditionnelles et inconditionnelles, mais la GRC ne dispose d'aucun processus pour supprimer les dossiers sur les condamnations injustifiées.

47. Comme dans le cas des réhabilitations, il est important de supprimer les dossiers relatifs à des condamnations injustifiées pour éviter de limiter les possibilités qu'ont les Canadiennes et Canadiens de travailler, de voyager, d'étudier ou de faire du bénévolat.

48. RECOMMANDATION

Afin d'atténuer le risque d'une communication illicite ou inappropriée, la GRC devrait instaurer des processus pour supprimer, selon les besoins, l'accès aux dossiers liés aux infractions ayant fait l'objet d'une réhabilitation ou aux condamnations injustifiées qui se trouvent dans la base de données du SIRP.

Réponse de la GRC :

La GRC adoptera immédiatement un processus et la technologie nécessaire pour isoler les renseignements liés aux personnes réhabilitées. En outre, la GRC modifiera les méthodes de fonctionnement normalisées du SIRP sur l'isolement d'information autre que les réhabilitations *en y ajoutant des directives sur le traitement des condamnations injustifiées.*

Les comptes d'utilisateur ne font l'objet d'aucun examen

49. Les contrôles d'accès sont des outils importants pour déterminer qui a accès à quelles données et quelles opérations les utilisateurs ont le droit de faire. Ces opérations peuvent comprendre la création, la lecture, la mise à jour ou la suppression de données. Nous avons examiné les contrôles d'accès instaurés par la GRC pour veiller à ce que les renseignements personnels du SIRP soient protégés convenablement.

50. Nous avons constaté que la GRC dispose de contrôles d'accès fondés sur les rôles en ce qui concerne la base de données du SIRP. Les niveaux d'accès sont établis en fonction des exigences du poste actuel de la personne. Toutefois, lorsque les utilisateurs du SIRP changent d'emploi, leurs droits d'accès ne sont pas toujours mis à jour ou révoqués en temps opportun.

51. La politique de la GRC concernant le SIRP stipule que le droit d'accès de l'utilisateur doit être supprimé s'il n'est plus nécessaire ou après quatorze mois d'inactivité. Pourtant, au cours de notre enquête, nous avons repéré plus de 1 000 utilisateurs dont les comptes actifs n'avaient pas servi depuis quatorze mois ou plus. La GRC n'a pas été en mesure de produire rapidement un rapport à jour et exact sur les utilisateurs et l'état de leur compte.

52. Si la GRC avait examiné l'activité des utilisateurs régulièrement, ces comptes auraient été désactivés. Le fait de laisser les droits d'accès aux utilisateurs qui ne sont plus autorisés à consulter le SIRP comporte un risque. Sans examens réguliers, il pourrait s'écouler un long moment avant que les consultations non autorisées soient découvertes.

53. RECOMMANDATION

La GRC devrait examiner régulièrement l'état des comptes d'utilisateur du SIRP et retirer l'accès s'il n'est plus nécessaire pour effectuer les tâches professionnelles.

Réponse de la GRC :

La GRC prendra immédiatement des mesures pour corriger la situation et examinera ses pratiques actuelles de formation des employés qui examinent les comptes d'utilisateur du SIRP.

54. **La capacité de surveiller les opérations des utilisateurs est limitée**. Nous avons examiné les capacités de journalisation des transactions dans le SIRP pour savoir si la GRC pouvait se pencher sur les incidents d'utilisation indue qui sont signalés. Le SIRP permet de faire le suivi des opérations des utilisateurs dans les journaux de vérification. Les renseignements enregistrés comprennent des détails sur les documents examinés et les modifications apportées.

55. La GRC nous a informés que, si une utilisation indue est soupçonnée, la quantité de travail nécessaire pour réunir et examiner les journaux de vérification limite la capacité de mener une enquête. Le SIRP comprend un outil permettant d'examiner automatiquement les journaux de vérification, mais il n'a pas été mis en place. Sans cette fonction, l'extraction des détails sur l'activité des utilisateurs est un travail très ardu. Il est donc difficile pour la GRC de faire enquête sur les mauvaises utilisations du système qui sont signalées.

56. RECOMMANDATION

Pour aider à mener des enquêtes sur la consultation non autorisée de renseignements personnels enregistrés dans le SIRP, la GRC devrait activer l'outil d'examen des journaux de vérification.

Réponse de la GRC :

La GRC activera immédiatement l'outil de consultation des journaux de vérification, qui est une méthode efficace pour réunir et examiner les entrées de ces journaux.

Le respect des politiques régissant l'utilisation des renseignements personnels ne fait pas systématiquement l'objet d'une vérification

57. En plus de la GRC, 23 services de police partenaires se servent du SIRP pour gérer leurs dossiers opérationnels. Nous avons examiné les politiques et les procédures de la GRC régissant l'utilisation du SIRP, les PE entre la GRC et les services de police partenaires et la façon dont la GRC veille à ce que les services de police respectent les modalités de ces ententes.

58. La GRC a établi des politiques et des procédures pour s'assurer que son utilisation du SIRP est conforme aux principes d'utilisation des renseignements personnels établis dans la *Loi sur la protection des renseignements personnels*. Elle fixe les conditions d'utilisation des PE avec tous les services de police partenaires pour que le système soit utilisé en conformité avec ces politiques et procédures.

59. Les PE comprennent des conditions sur l'utilisation et la diffusion acceptables des renseignements contenus dans le SIRP, des clauses sur la sécurité, des exigences en matière de formation, des procédures de signalement des incidents et des protocoles pour faire en sorte que les renseignements contenus dans le SIRP soient utilisés à des fins légitimes d'application de la loi.

60. À moins d'une résiliation, les PE sont en vigueur pendant cinq ans à partir de la date de la signature. Les motifs de résiliation comprennent l'utilisation et la communication sans autorisation, tout incident lié aux politiques ou règlements sur la sécurité et la violation de la politique de la GRC concernant le SIRP.

61. En examinant les PE, nous avons constaté que des clauses permettent à la GRC de mener des vérifications sur les organismes pour s'assurer qu'ils respectent les modalités. La GRC a le droit de surveiller l'utilisation de ses réseaux, y compris par des employés précis, et de mener des examens de sécurité périodiques en visitant les locaux des services de police partenaires. Les vérifications de l'utilisation du SIRP sont importantes puisqu'elles garantissent à la GRC que les utilisateurs respectent les procédures régissant l'utilisation des renseignements personnels du SIRP.

62. La GRC n'a pu démontrer qu'elle entreprend systématiquement des examens auprès des services de police partenaires pour veiller à ce que les renseignements personnels du SIRP soient utilisés en conformité avec les modalités applicables. Une quantité limitée de vérifications ont été entreprises. Par exemple, tous les services de police partenaires de l'Alberta, mais seulement quelques-uns de la Nouvelle-Écosse et aucun de l'Île-du-Prince-Édouard, n'ont fait l'objet d'une vérification. De plus, la GRC n'a pu prouver qu'elle examinait systématiquement ses propres utilisateurs.

63. RECOMMANDATION

La GRC devrait adopter un processus d'examen régulier fournissant l'assurance que tous les utilisateurs respectent les politiques et les procédures régissant l'utilisation des renseignements personnels enregistrés dans le SIRP.

Réponse de la GRC :

La GRC examinera immédiatement son processus de vérification actuel et apportera des modifications au besoin de façon à ce que les utilisateurs du SIRP, tant à l'interne qu'à l'externe, fassent l'objet d'examens.

Conclusion

64. La GRC a élaboré et mis en œuvre des politiques et des procédures pour protéger les renseignements personnels des Canadiennes et Canadiens qui sont consultés dans la base de données du CIPC. Des atteintes à la protection des renseignements personnels ont eu lieu, mais relativement rarement. En outre, des mécanismes sont en place pour enquêter sur ces atteintes et prendre des mesures à la suite des enquêtes. La GRC a établi des PE pour régir l'utilisation du CIPC par les organismes dont les pouvoirs d'application de la loi sont limités ou qui jouent des rôles complémentaires dans le cadre de l'application de la loi. Toutefois, la GRC n'a pas encore conclu de PE officiel avec environ 25 % des services de police ayant accès au CIPC.

65. Des vérifications sont régulièrement effectuées pour examiner les enquêtes de sécurité sur le personnel et la sécurité sur le terminal et le site à interface du CIPC, ainsi que pour veiller à ce que tous les organismes, dont la GRC, respectent la politique et les lignes directrices du Manuel de référence du CIPC. Ce système de surveillance vise à faire en sorte que tous les utilisateurs respectent les principes de protection des renseignements personnels énoncés dans la politique du CIPC.

66. La GRC a élaboré des politiques et des procédures d'exploitation normalisées qui indiquent pendant combien de temps les renseignements peuvent être conservés dans le SIRP avant d'être isolés ou supprimés. Cependant, les renseignements personnels sont conservés plus longtemps qu'il est nécessaire, contrairement aux dispositions de la *Loi sur la protection des renseignements personnels*. En outre, la GRC ne dispose d'aucun processus pour supprimer l'accès aux dossiers liés aux condamnations ayant fait l'objet d'une réhabilitation ou aux condamnations injustifiées. Il est important pour les Canadiennes et Canadiens réhabilités ou condamnés injustement que de tels renseignements ne soient pas communiqués de façon inopportune, car cela pourrait nuire à leurs chances d'obtenir un emploi, de voyager, d'étudier ou de faire du bénévolat comme tout autre Canadienne ou Canadien.

67. Aucun examen actif des comptes d'utilisateurs du SIRP n'est effectué. La politique de la GRC sur le SIRP stipule que le droit d'accès d'un utilisateur doit être révoqué si celui ci n'en a plus besoin pour exécuter ses tâches professionnelles ou après 14 mois d'inactivité, mais nous avons vu que plus de 1 000 utilisateurs ayant un compte actif n'avaient pas consulté le SIRP depuis 14 mois ou plus. Nous avons aussi constaté que le processus d'examen de l'activité des utilisateurs du SIRP est lourd, ce qui complique les enquêtes sur les mauvais usages du système.

68. La GRC n'a pas été en mesure de démontrer qu'elle examine systématiquement les utilisateurs du SIRP pour s'assurer que les renseignements personnels sont utilisés en conformité avec les politiques en vigueur.

69. La GRC gère adéquatement les renseignements personnels du CIPC, mais elle devrait établir un échéancier clair concernant l'établissement de PE, comprenant des clauses sur la protection des renseignements personnels, avec tous les services de police.

70. La GRC doit améliorer la gestion des renseignements personnels enregistrés dans la base de données du SIRP. Elle doit supprimer des données qui se trouvent dans le système, mettre en œuvre des processus pour supprimer l'accès aux dossiers concernant les infractions ayant fait l'objet d'une réhabilitation et les condamnations injustifiées, examiner régulièrement l'état des comptes d'utilisateur du SIRP et désactiver l'accès lorsqu'il n'est plus nécessaire pour assumer des tâches professionnelles, activer l'outil d'examen des journaux de vérification du SIRP et adopter un processus d'examen régulier fournissant l'assurance que tous les utilisateurs respectent les politiques et les procédures régissant l'utilisation des renseignements personnels enregistrés dans le SIRP.

À propos de la vérification

POUVOIR

L'article 37 de la *Loi sur la protection des renseignements personnels* confèreà la commissaire à la protection de la vie privée le pouvoir d'examiner les pratiques de traitement des renseignements personnels utilisées par les institutions fédérales.

OBJECTIF

La vérification visait à déterminer si la GRC gère adéquatement les renseignements personnels contenus dans les bases de données du CIPC et du SIRP.

CRITÈRES

Les critères de la vérification découlent de la *Loi sur la protection des renseignements personnels*. Les mécanismes de contrôle soutenant la technologie de l'information (TI) ont été évalués à l'aide de critères tirés des Control Objectives for Information and Related Technology (COBIT), une norme de l'industrie qui établit les pratiques exemplaires en matière de gestion de la TI, ainsi que des politiques et des normes pertinentes du gouvernement du Canada.

Nous nous attendions à ce que la GRC :

- ait établi des politiques et des procédures pour régir l'accès au CIPC et son utilisation;
- surveille l'utilisation du CIPC pour garantir le respect des conditions d'utilisation;
- ait établi des politiques et des procédures pour supprimer du SIRP les renseignements personnels qui ne sont plus nécessaires;
- gère adéquatement l'accès au SIRP;
- surveille l'utilisation du SIRP pour garantir le respect de ses politiques et de ses procédures visant à protéger les renseignements personnels.

PORTÉE ET DÉMARCHE

Nous avons examiné les politiques, les systèmes, les mesures de protection et les contrôles administratifs relatifs au CIPC et au SIRP que la GRC emploie pour régir l'utilisation, la communication, la conservation et l'élimination des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels*.

Les éléments probants ont été obtenus en examinant divers documents sur le déroulement des opérations, les procédures de fonctionnement normalisées, les ententes, les calendriers de conservation des documents, les documents relatifs aux programmes, les rapports de vérification ainsi que sur les dossiers et contrôles d'application. Nous avons également passé en revue les contrôles d'accès des utilisateurs et l'architecture de système du CIPC et du SIRP en plus de demander des rencontres, des démonstrations et des visites guidées pour appuyer notre travail de vérification.

Nous n'avons pas examiné comment les renseignements contenus dans ces bases de données influaient sur les décisions prises dans le cadre des activités quotidiennes de la GRC. De plus, la vérification n'a porté que sur les mesures de sécurité prises par la GRC et non sur celles d'autres utilisateurs du CIPC et du SIRP.

Le travail de vérification était pratiquement terminé le 31 mars 2011.

NORMES

La vérification a été effectuée en conformité avec les pratiques, les politiques et le mandat législatif du Commissariat à la protection de la vie privée du Canada et respectait l'esprit des normes de vérification recommandées par l'Institut canadien des comptables agréés.

ÉQUIPE DE VÉRIFICATION

Directeur général : Steven Morgan

Sylvie Gallo Daccash
Anne Overton
Bill Wilson

Appendice : Liste de recommandations

1. RECOMMANDATION

Le CIPC devrait établir un échéancier clair concernant l'établissement de PE, comprenant des clauses sur la protection des renseignements personnels, avec tous les services de police.

Réponse de la GRC :

Comme l'a demandé le sous-commissaire, Soutien aux services de police, en novembre 2010, le CIPC négocie activement avec les derniers services de police (25 %) qui n'ont pas encore signé de PE. Comme prévu, le modèle de PE ne s'applique pas nécessairement dans tous les cas et les différences font l'objet de discussions pour que des PE soient conclus d'ici le 31 mars 2012.

2. RECOMMANDATION

La GRC devrait éliminer les données du SIRP qui doivent l'être de façon à respecter la *Loi sur la protection des renseignements personnels*.

Réponse de la GRC :

La GRC est d'accord et prendra immédiatement des mesures pour corriger la situation.

3. RECOMMANDATION

Afin d'atténuer le risque d'une communication illicite ou inappropriée, la GRC devrait instaurer des processus pour supprimer, selon les besoins, l'accès aux dossiers liés aux infractions ayant fait l'objet d'une réhabilitation ou aux condamnations injustifiées qui se trouvent dans la base de données du SIRP.

Réponse de la GRC :

La GRC adoptera immédiatement un processus et la technologie nécessaire pour isoler les renseignements liés aux personnes réhabilitées. En outre, la GRC modifiera les méthodes de fonctionnement normalisées du SIRP sur *l'isolement d'information autre que les réhabilitations* en y ajoutant des directives sur le traitement des condamnations injustifiées.

4. RECOMMANDATION

La GRC devrait examiner régulièrement l'état des comptes d'utilisateur du SIRP et retirer l'accès s'il n'est plus nécessaire pour effectuer les tâches professionnelles.

Réponse de la GRC :

La GRC prendra immédiatement des mesures pour corriger la situation et examinera ses pratiques actuelles de formation des employés qui examinent les comptes d'utilisateur du SIRP.

5. RECOMMANDATION

Pour aider à mener des enquêtes sur la consultation non autorisée de renseignements personnels enregistrés dans le SIRP, la GRC devrait activer l'outil d'examen des journaux de vérification.

Réponse de la GRC :

La GRC activera immédiatement l'outil de consultation des journaux de vérification, qui est une méthode efficace pour réunir et examiner les entrées de ces journaux.

6. RECOMMANDATION

La GRC devrait adopter un processus d'examen régulier fournissant l'assurance que tous les utilisateurs respectent les politiques et les procédures régissant l'utilisation des renseignements personnels enregistrés dans le SIRP.

Réponse de la GRC :

La GRC examinera immédiatement son processus de vérification actuel et apportera des modifications au besoin de façon à ce que les utilisateurs du SIRP, tant à l'interne qu'à l'externe, fassent l'objet d'examens.