RAPPORT DE VÉRIFICATION

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE CADRE DE LA RÉALISATION DU PLAN D'UTILISATION DES FICHIERS GOUVERNEMENTAUX AU MINISTÈRE DU REVENU DU QUÉBEC

DÉCEMBRE 2001

TABLE DES MATIÈRES

INTRODUCTION

Le présent rapport de vérification vise à répondre à la demande de la Commission d'accès à l'information (Commission) de réaliser une « vérification de la conformité quant au respect de la protection des renseignements personnels dans le cadre de la réalisation du plan d'utilisation des fichiers gouvernementaux » au ministère du Revenu du Québec (MRQ). Les réponses apportées par le vérificateur à ces préoccupations proviennent de l'observation directe des faits de même que de l'analyse des informations issues des discussions tenues et des documents obtenus sur place, de janvier à mai 2001.

Les travaux réalisés ont consisté à examiner les principaux éléments d'organisation du travail et de sécurité reliés à l'obtention et à la protection des renseignements externes mis en place par le MRQ à la suite des modifications apportées à l'article 71 de la *Loi sur le ministère du Revenu*, ci-après appelée la Loi, par le projet de loi n^{o} 32 adopté en juin 1996.

Le premier volet de la vérification a porté sur le plan d'utilisation prévu à l'article 71.0.3 de la Loi. Il consiste en une analyse des étapes menant à l'établissement de ce plan. La seconde partie de ce volet est en fait un examen des principaux systèmes et contrôles mis en place pour assurer le suivi et le respect de ce même plan. Enfin, une dernière partie contient des informations au sujet du projet « profil de richesse », et ce, dans le but d'évaluer sommairement les risques qu'il représente pour la protection des renseignements personnels et confidentiels des Québécois.

Le second volet a été axé sur la sécurité et la protection des renseignements externes obtenus. Le vérificateur a d'abord examiné quelques éléments reliés à la sécurité des postes de travail des utilisateurs de la centrale de données. Il a ensuite analysé les principaux contrôles mis en place au MRQ concernant la gestion des accès aux renseignements externes, la journalisation de ceux-ci et, finalement, la gestion des extrants. Les contrôles dont il est question ici sont ceux visant à gérer et à rendre compte des accès autorisés aux renseignements et des contrôles exercés sur les fichiers et documents résultant de ces accès.

Il est très important de retenir que les travaux de vérification réalisés pour ce second volet ne peuvent en aucun temps être assimilés à une vérification exhaustive de la sécurité de l'environnement informatique de la centrale de données[1]. La présente vérification ne permet donc pas de s'assurer de l'existence et de l'efficacité des mesures destinées à détecter et à empêcher les accès non autorisés aux renseignements contenus dans la centrale de données.

Le troisième et dernier volet de la présente vérification a consisté en un examen sommaire des mécanismes d'information disponibles au MRQ et permettant d'identifier, de comptabiliser et de rendre compte des revenus découlant de la cueillette des renseignements provenant des fichiers externes obtenus. La prise de connaissance relative à ce sujet a été effectuée principalement auprès du personnel de la Direction de la comptabilisation des revenus qui est l'utilisateur principal du système appelé « Portrait ministériel des revenus » (PMR). Une discussion avec une personne responsable à la Direction générale adjointe de la recherche fiscale (DGARF) a également eu lieu pour explorer globalement les avantages reliés à la mise en place d'un

[1] La centrale de données est un entrepôt de données développé spécifiquement « pour assurer la réalisation des objectifs du *Plan de lutte contre l'évasion fiscale et le travail au noir* ».

mécanisme permettant éventuellement de rendre compte du rendement découlant de l'obtention de renseignements externes par le MRQ.

1. LE PLAN D'UTILISATION

1.1 Le plan d'utilisation initial et ses mises à jour

L'article 71.0.3 de la Loi édicte que « *le ministre dresse un plan d'utilisation de tout fichier de renseignements qu'il entend obtenir en vertu de l'article 71 à des fins de comparaison, de couplage ou d'appariement et le soumet pour avis à la Commission d'accès à l'information* ».

Cet article décrit le contenu de ce plan d'utilisation, à savoir que « *le plan d'utilisation comprend une brève description :*

a) des fichiers de renseignements demandés et de leur provenance;
b) des finalités recherchées;
c) de l'usage projeté;
d) des modalités d'échange et, le cas échéant,
e) des mesures de sécurité.

La Commission d'accès à l'information émet un avis sur ce plan dans les 30 jours de la réception de celui-ci ».

Le plan d'utilisation constitue donc, de par son contenu, un document de référence essentiel tant au moment de la cueillette qu'au moment de l'autorisation des accès et de l'utilisation subséquente des renseignements obtenus.

Tout d'abord, mentionnons que le plan d'utilisation est élaboré en tenant compte, dans un premier temps, du plan stratégique du MRQ. Ce document permet, entre autres, de connaître les actions envisagées par le MRQ pour réaliser sa mission en matière de lutte contre l'évasion fiscale.

Dans un second temps, chaque unité concernée en cette matière produit un document appelé « plan tactique » où l'on retrouve les éléments correspondant à un effort pour contrer l'évasion fiscale et le travail au noir. Au sein de ces unités, il existe ce qu'il est convenu d'appeler des groupes de demandeurs primaires. Il s'agit de personnes impliquées dans la réalisation des travaux de recherche et de développement portant sur les stratagèmes utilisés par des contribuables ou des entreprises pour éviter de payer des taxes et des impôts.

Les principaux groupes de demandeurs primaires se retrouvent au Bureau de lutte contre l'évasion fiscale (BLEF) de la DGARF, à Québec et à Montréal. Actuellement, on en retrouve aussi quelques-uns à la Direction générale de la capitale et des régions (DGCAR) et à la Direction générale de la métropole (DGMET).

Cependant, il est à noter que le BLEF demeure le principal groupe de demandeurs primaires depuis le début de la période d'intensification de la lutte contre l'évasion fiscale en 1996. À ce

titre, il est à l'origine de l'inscription de la plus grande partie des fichiers de renseignements, des finalités recherchées ainsi que des usages projetés figurant au plan d'utilisation initial et à ses mises à jour.

En pratique, le bureau du BLEF, à Québec, assure la coordination de la lutte contre l'évasion fiscale à la fois pour le bureau de Québec et pour celui de Montréal. Une personne de ce bureau assume la fonction visant à s'assurer que seulement les projets correspondant aux orientations stratégiques et aux plans tactiques approuvés sont acheminés au responsable du plan d'utilisation à la Direction de la gestion de l'information (DGI).

L'établissement du plan d'utilisation

La DGI de la DGARF est responsable de l'établissement du plan d'utilisation.

Le coordonnateur du plan d'utilisation à la DGI est la personne qui exerce les principales tâches permettant d'assurer la conformité des demandes d'obtention de types de fichiers externes. Il doit donc s'assurer que les renseignements apparaissant au plan d'utilisation initial et à ses mises à jour respectent les dispositions de la Loi et, en particulier, celle du premier alinéa de l'article 71, où l'on retrouve le texte suivant : « *Tout organisme public au sens de l'article 31.1.4,… doit fournir au ministre tout renseignement que celui-ci indique, lorsque ce renseignement est nécessaire à l'application et à l'exécution d'une loi fiscale* ».

Il est important de souligner qu'au niveau du plan d'utilisation, les finalités recherchées et les usages projetés sont formulés en termes génériques et ne fournissent qu'un aperçu minimal des projets et activités spécifiques ayant mené à l'inscription d'un type de fichier au plan d'utilisation. Ainsi, le plan d'utilisation permet d'identifier la provenance des renseignements que le MRQ envisage d'obtenir, mais ne contient pas d'informations précises concernant les fichiers et les éléments d'information, aussi appelés « variables », qui seront réellement demandés et obtenus des fournisseurs impliqués.

En effet, les éléments d'information requis concernant les contribuables ou entreprises sont très rarement identifiés de façon précise lors de l'inscription d'un type de fichier au plan d'utilisation; ces variables font surtout l'objet de travaux par les analystes de la DGI impliqués au moment de l'obtention et de la réception des fichiers externes, en collaboration avec les analystes des demandeurs primaires.

Soulignons aussi qu'un même fichier peut être utilisé dans plusieurs projets et activités. Ceci est vrai tout particulièrement pour les fichiers dits « de type horizontal ». Par exemple, un fichier reçu de la Société de l'assurance automobile du Québec (SAAQ) sert aussi bien dans les projets de lutte reliés spécifiquement au secteur de l'automobile que dans le projet horizontal « profil de richesse ».

CONSTATATIONS

Après analyse des informations apparaissant au plan d'utilisation, il appert que la précision des libellés actuels ne permet pas de bien distinguer les diverses utilisations possibles des renseignements externes que l'on veut obtenir. En effet, le niveau de connaissance des projets sous-jacents qu'il est possible de retirer de la simple lecture du plan d'utilisation est le plus souvent minimal. De plus, il y a une grande redondance au niveau des textes présentant les finalités recherchées et les usages projetés. Donc, de l'avis du vérificateur, le plan d'utilisation est, dans sa forme actuelle, « flou », et ce, principalement au niveau du texte décrivant l'usage projeté correspondant à chacun des types de fichiers demandés.

À titre d'exemple, au plan d'utilisation actuel, pour le fichier des bénéficiaires de la Régie de l'assurance maladie du Québec, la finalité recherchée se lit comme suit : « *Pour détecter les individus qui n'ont pas produit de déclaration de revenus* ». Quant à l'usage projeté, on retrouve le même texte que pour la plupart des autres types de fichiers inscrits au plan d'utilisation, à savoir « *Le ministère effectuera des comparaisons de ce fichier avec ceux dont il dispose et ceux dont il disposera pour extraire les dossiers irréguliers. Ces cas seront vérifiés afin de valider les résultats de la comparaison.* ». Ce texte est lui-même suivi d'un autre, lui aussi standard, décrivant sommairement la comparaison envisagée pour rechercher les cas de délinquance de déclaration des individus et donnant un aperçu de la comparaison envisagée, entre autres, pour le projet appelé « Profil de richesse ». Le lecteur du présent rapport trouvera, en annexe, quelques extraits du plan d'utilisation illustrant la redondance des textes employés.

Selon le vérificateur, il est difficile de vérifier, sans disposer d'éléments d'information supplémentaires, si les projets de lutte contre l'évasion fiscale réalisés étaient inscrits comme tels au plan d'utilisation approuvé. En effet, le lien entre les projets de lutte contre l'évasion fiscale et le plan d'utilisation est souvent difficile à reconstituer. Ainsi, seules des personnes œuvrant à l'interne et impliquées de près dans les activités de lutte contre l'évasion fiscale pourraient effectuer une vérification adéquate sur cette question.

Le plan d'utilisation n'est donc pas suffisant en lui-même pour assurer la réalisation d'analyses approfondies ou l'exercice de contrôles éventuels par des intervenants internes ou externes au MRQ et visant à se prononcer sur le caractère nécessaire des fichiers externes obtenus. Des connaissances additionnelles sont requises pour exercer un contrôle réel sur l'obtention et l'utilisation des fichiers jugés nécessaires à la réalisation des projets de lutte contre l'évasion fiscale. La même situation existe pour ce qui concerne les éléments d'information (variables) obtenus des fournisseurs de renseignements externes.

RECOMMANDATION 1

Un plan d'utilisation renouvelé ou tout autre document contenant les informations supplémentaires nécessaires aux personnes devant assurer un rôle de surveillance au regard de l'établissement et du respect du plan d'utilisation devrait être produit et mis à leur disposition.

De l'avis du vérificateur, on devrait retrouver, au moins dans la partie confidentielle du plan d'utilisation ou dans tout autre document officiel disponible à des fins de contrôle, une description complète des éléments d'information que le MRQ désire obtenir ainsi qu'une présentation détaillée de ce qu'il veut en faire concrètement. La formulation adoptée pour la description de l'usage projeté devrait permettre d'éviter que les textes utilisés ouvrent la porte à une interprétation trop libérale aux divers usages possibles des fichiers externes obtenus.

En effet, vu qu'il constitue le principal élément formel disponible sur lequel peuvent s'appuyer les personnes responsables de l'application du plan d'utilisation approuvé, le texte apparaissant à ce dernier devrait être assez clair pour permettre aux employés de la DGI et aux autres intervenants, occupant une fonction de contrôle visant à s'assurer de la conformité des gestes concrets posés avec le plan d'utilisation autorisé, d'effectuer leur travail efficacement. Plus précisément, le texte décrivant les finalités recherchées et, plus particulièrement, celui placé au niveau de l'usage projeté devrait être assez explicite pour que les personnes qui ont un rôle de surveillance à jouer puissent réaliser pleinement leur mission pour chacun des fichiers de renseignements à obtenir.

D'autre part, vu l'importance des liens à établir entre le plan d'utilisation et les accès aux données externes obtenues, le texte apparaissant à ce document devrait permettre aux gestionnaires et aux autres personnes impliquées d'attribuer les profils d'accès en conformité avec les projets de lutte contre l'évasion fiscale nécessitant l'accès à ces données.

COMMENTAIRES DU MRQ

> « *Le plan d'utilisation consigne les besoins en fichiers de renseignements externes du ministère du Revenu pour des activités qui sont en grande partie à l'étape de la planification. Lorsque le Ministère en prépare une mise à jour, il collige des informations additionnelles sur la nature des projets qui requièrent des renseignements externes. Ces informations, confidentielles en vertu de l'article 71.0.5 LMR, servent notamment à préparer des documents complémentaires acheminés à la Commission pour appuyer la mise à jour. Elles constituent par la suite l'une des références pour contrôler les droits d'accès aux fichiers obtenus.*
>
> *La Commission reçoit annuellement le détail des nouveaux éléments d'information obtenus pour chaque fichier inscrit au plan. Le Ministère rend également des comptes sur les travaux réalisés dans le rapport d'activité prévu à l'article 71.0.6 LMR. Ce rapport est déposé annuellement à l'Assemblée nationale depuis 5 ans et comprend un avis de la Commission.*
>
> *Bien que le plan d'utilisation n'a pas pour objet de contenir toutes les informations souhaitées par le vérificateur, le Ministère projette d'en clarifier certaines notions dans une prochaine mise à jour afin d'en faciliter la lecture et la compréhension, dans le sens indiqué par la Commission.* »

RÉACTION AUX COMMENTAIRES

Cette recommandation visait les besoins tant à l'interne qu'à l'externe au niveau des intervenants jouant un rôle de surveillance, principalement à la DGI. Les commentaires du MRQ ne portent que sur les informations acheminées à la Commission à diverses étapes du plan d'utilisation.

1.2 Le suivi et le respect du plan d'utilisation

1.2.1 Le processus d'obtention, de réception ainsi que de destruction des fichiers

Le processus d'obtention et de réception des fichiers

Des analystes de la DGI se sont vu attribuer, pour l'une et l'autre de ces deux premières étapes, la responsabilité de traiter avec un ou plusieurs ministères ou organismes fournisseurs de renseignements en vertu de l'article 71 de la Loi.

Chacun de ces analystes est responsable des démarches auprès de fournisseurs spécifiques et il évalue la demande d'extraits de fichiers attendue de ceux-ci. Ce travail est souvent réalisé avec la participation d'un analyste travaillant pour le ou les demandeurs primaires impliqués dans la demande concernant le type de fichier externe en cause. Les analystes de la DGI déterminent aussi les variables correspondant aux besoins des utilisateurs (BLEF, DGCAR et DGMET) en cause, en fonction des finalités recherchées et des usages projetés apparaissant au plan d'utilisation. Les analystes de la DGI jouent donc un rôle de surveillance pour ce qui est du respect du plan d'utilisation.

Pour ce qui concerne le projet « Profil de richesse », les analystes de la DGI travaillent uniquement sur la base des fichiers détenus par les ministères et organismes qui font partie de leur champ de spécialisation. En conséquence, les fichiers nécessaires à l'établissement des indices de richesse provenant de divers fournisseurs, plusieurs analystes de la DGI sont appelés à travailler à l'obtention des fichiers requis par ce projet horizontal. Les analystes de la DGI suivent un processus qui n'est pas directement affecté par les projets qui sont eux-mêmes à la source de l'inscription des fichiers au plan d'utilisation. Le projet « Profil de richesse » est donc transparent pour les analystes de la DGI, responsables de l'obtention et de la réception des fichiers requis.

Le processus de destruction des fichiers

Chacun des analystes de la DGI impliqués dans le processus d'obtention et de réception d'un fichier donné est aussi responsable du processus de destruction, physique et logique, des fichiers reçus ainsi que des extrants en découlant. Cette action vise surtout à assurer le respect du calendrier de destruction approuvé par la Commission. Pour le bénéfice du lecteur, il convient de rappeler que le BLEF, à Québec et à Montréal, est la principale entité ministérielle impliquée lors de l'inscription et de la radiation de types de fichiers, de même que pour la description des finalités recherchées et de l'usage projeté.

D'autre part, le MRQ est actuellement en période de rationalisation en rapport avec les projets de lutte contre l'évasion fiscale, ce qui amène le retrait de fichiers externes qui ne sont plus ou pas requis; les fichiers identifiés comme n'étant plus nécessaires en fonction des critères établis sont eux aussi détruits selon le processus en place. En ce sens, les équipes du BLEF ont déjà effectué un travail important pour identifier les projets à conserver. Les résultats de ce travail ont été acheminés au coordonnateur du plan d'utilisation à la DGI pour être pris en considération au niveau de la prochaine mise à jour de ce plan. D'après ce dernier, le même exercice a été effectué par les équipes correspondantes au sein des autres groupes de demandeurs primaires du MRQ. L'objectif poursuivi est de s'assurer que les interventions de lutte contre l'évasion fiscale s'arriment avec les projets prioritaires du MRQ en cette matière.

Au niveau de la DGI, un dossier physique sous format papier est actuellement constitué pour chaque ronde de destruction de façon à s'assurer de l'intégrité du processus de destruction mis en place. En pratique, l'analyste responsable s'appuie habituellement sur une extraction du système de gestion des fichiers (SGF) obtenue en fonction de la date de fin inscrite au plan d'utilisation.

Des informations spécifiques à la gestion des extrants, processus qui vise surtout à assurer la destruction des fichiers obtenus, apparaissent au second volet du présent rapport.

CONSTATATION

La qualité des travaux visant à assurer le respect du plan d'utilisation initial et de ses mises à jour repose sur le travail et les connaissances acquises par chacun des analystes de la DGI, auxquels sont attribuées des tâches impliquant un rôle de surveillance.

RECOMMANDATION 2

Vu l'importance stratégique des fonctions des analystes de la DGI pour assurer le respect du plan d'utilisation, le MRQ devrait développer dès que possible les documents, guides de travail et autres outils nécessaires au personnel de la DGI assumant des tâches impliquant un rôle de surveillance. Ceci permettrait d'appuyer concrètement leurs efforts en vue d'assumer pleinement ce rôle primordial.

COMMENTAIRES DU MRQ

> « *Les rôles principaux en matière de contrôle du plan d'utilisation sont exercés par les responsables mentionnés dans les directives internes d'administration (" DIA ") touchant à la protection des renseignements externes, soit la DIA-10 sur les profils d'utilisateurs de la Centrale de données et la DIA-11 sur la gestion des documents et fichiers dérivés des fichiers du plan d'utilisation. Il y est prévu que le gestionnaire de la Direction de la gestion de l'information (" DGI ")*

s'assure de la conformité de l'usage des renseignements annoncé lors de l'octroi des privilèges d'accès, coordonne la reddition de comptes sur l'utilisation de ces renseignements et coordonne leur destruction.

Le rôle des analystes de la DGI est surtout de procéder à la demande des fichiers inscrits au plan d'utilisation et d'en effectuer le traitement en vue de les rendre disponibles aux utilisateurs. À cet effet, un guide sommaire leur est destiné. La DGI procède actuellement à la révision de ses processus ainsi que des documents qui les supportent. La recommandation de la Commission sera prise en compte au cours de l'exercice pour ce qui est des aspects de leur tâche pouvant toucher à la surveillance. »

1.2.2 Le système de gestion des fichiers

Outre l'établissement du plan d'utilisation, la DGI de la DGARF s'assure aussi du respect du plan d'utilisation après son approbation par les autorités tant ministérielles que gouvernementales. Cette direction a aussi un rôle majeur à jouer lors de la reddition de comptes inscrite à l'article 71 et suivants de la Loi. Il s'agit principalement ici de la production des rapports d'activité au 31 mars de chaque année.

Après l'approbation du plan d'utilisation, la DGI est responsable de la mise à jour du SGF. Ce système sert principalement au suivi des travaux à effectuer pour compléter les étapes d'obtention et de réception des fichiers. Ainsi, dès la réception des fichiers, les analystes de la DGI mettent le SGF à jour.

De plus, le SGF permet de connaître, entre autres, l'état de situation concernant la réception de chacun des types de fichiers inscrits au plan d'utilisation initial ou à une mise à jour subséquente de même que le nombre réel d'extraits de fichiers reçus en rapport avec un type de fichier donné.

Une autre fonction importante du SGF est qu'il est aussi utilisé pour déclencher le processus de rafraîchissement des fichiers qui est effectué selon la fréquence prévue aux modalités d'échange apparaissant au plan d'utilisation.

Soulignons que, lors d'un rafraîchissement, le nombre de variables obtenues peut varier sensiblement. Cette variation est habituellement due à la connaissance acquise, à l'interne du MRQ, à la suite de la réception de l'extrait de fichier initial. En effet, l'expertise des analystes de la DGI se développe avec l'usage des extraits de fichiers, tout comme celle des utilisateurs. Cette variation peut aussi être due au besoin d'accéder à un niveau de détails supplémentaires ou à des variables complémentaires disponibles auprès du fournisseur.

D'autre part, le SGF contribue à assurer la fiabilité du processus de destruction en ce sens qu'une liste des fichiers à détruire est produite par ce système afin de supporter la préparation du calendrier de destruction. À la fin du processus de destruction, les informations pertinentes sont colligées dans le SGF pour documenter la destruction effectuée.

Il est à noter que les fichiers concernant des transactions s'échelonnant sur plusieurs années sont, autant que possible, subdivisés en fonction des années civiles en cause, et ce, dès leur réception. Cette procédure vise à faciliter le respect du calendrier de destruction approuvé par la Commission.

Une fois le calendrier de destruction établi, la personne de la DGI qui coordonne la destruction des fichiers recueille, auprès des utilisateurs des renseignements externes et dans les registres de gestion des extrants auxquels elle a accès, la liste des extrants en circulation. Ceci permet, le moment venu, d'adresser aux personnes responsables une demande formelle de destruction de renseignements externes précisant les extraits de fichiers qu'ils ont eu en leur possession et qu'ils doivent détruire. Le document en question comporte aussi des informations concernant la destruction des extrants générés à partir des fichiers identifiés ainsi que la définition des données externes devenues fiscalisées. Un formulaire d'attestation spécifique à la demande de destruction est joint en annexe à cette demande. Ce formulaire doit être retourné, dûment rempli, à l'analyste de la DGI en cause.

La DGI se charge des producteurs d'extrants, soit le premier niveau de la clientèle de la centrale de données. Pour leur part, les producteurs doivent s'occuper de coordonner la destruction chez leurs demandeurs d'extrants. Ce point de contrôle sera traité dans le deuxième volet du présent rapport, au niveau de la gestion des extrants.

En ce qui concerne les « données externes devenues fiscalisées »[2] telles que définies par le MRQ, le SGF n'accumule aucune information sur ce sujet. L'impact de ces données se situe au niveau du processus de destruction, principalement lors du déclenchement des rondes de destruction. Le SGF ne permet donc en aucune façon de rendre compte de la situation réelle en ce qui concerne les « données externes devenues fiscalisées ».

Il faut se pencher sur la gestion des extrants pour se faire une idée de cette réalité que représente la non-destruction des données devenues fiscalisées. Ainsi, c'est seulement au niveau des utilisateurs des unités opérationnelles qu'on peut obtenir des informations sur le nombre et la proportion de ces données, le moment où la « fiscalisation » se produit en réalité, les mécanismes mis en place pour assurer leur conservation adéquate ainsi que la gestion de l'accès à celles-ci et la protection des renseignements externes.

CONSTATATIONS

Le SGF représente un actif majeur pour soutenir les personnes dont le rôle est d'assurer la conformité de l'obtention et de l'utilisation des extraits de fichiers reçus avec le plan d'utilisation approuvé.

[2] Selon la définition du MRQ apparaissant à la page 16 du rapport d'activité au 31 mars 2001, les données externes devenues fiscalisées sont celles incluses aux dossiers des contribuables ou des mandataires acheminées aux unités de récupération fiscale et faisant l'objet d'une vérification ou d'une nouvelle cotisation; ce sont aussi celles qui sont intégrées dans certains systèmes opérationnels du MRQ à titre de données référentielles d'identification, notamment l'adresse, le numéro de téléphone et le numéro d'assurance sociale.

La plupart des fonctionnalités du SGF sont actuellement disponibles. Cependant, au moment de notre vérification sur place, quelques-unes des fonctionnalités prévues dans la section « requêtes particulières » étaient encore au stade du développement informatique.

Certaines de celles-ci permettraient d'automatiser la production de rapports présentant un intérêt, soit pour la gestion interne des renseignements obtenus à la suite de l'adoption du plan d'utilisation, soit pour la Commission, soit pour tout autre intervenant externe qui y aurait légalement droit. À titre d'exemple, l'une de ces fonctionnalités vise la production d'un « registre des fichiers détruits à la Commission ».

1.2.3 L'obtention réelle des fichiers inscrits au plan d'utilisation

Lors de la vérification sur place, le vérificateur a obtenu des informations compilées à partir des données disponibles au SGF en février 2001. Ce dernier a pu, par la suite, établir des statistiques concernant la réception des types de fichiers inscrits au plan d'utilisation initial ainsi qu'à chacune des mises à jour de ce plan d'utilisation approuvées de même que concernant le nombre d'extraits de fichiers correspondants[3]. Les extraits de fichiers dont il est question ici sont en fait le ou les fichiers qui, en pratique, permettent au ministère ou à l'organisme détenteur des informations de satisfaire la demande du MRQ. Le nombre d'extraits de fichiers requis pour répondre à une demande du MRQ dépend surtout de l'organisation des données dans les systèmes informatiques du fournisseur en cause.

CONSTATATIONS

En ce qui concerne le plan d'utilisation de juillet 1996, le vérificateur constate que sur les 71 types de fichiers inscrits, le MRQ n'en avait reçu que 43. Il appert aussi que ces 43 types de fichiers ont donné lieu à la réception de 170 extraits de fichiers. Ceci illustre la distinction entre un « type de fichier » et un « extrait de fichier » ainsi que le fait, pour un type de fichier inscrit à ce plan d'utilisation, que le MRQ a reçu, assez souvent, plus d'un extrait de fichiers du fournisseur de renseignements en cause. Par exemple, le type de fichier inscrit pour obtenir les renseignements sur l'immatriculation des véhicules routiers au Québec a donné lieu à la réception de 21 extraits de fichiers en provenance de la SAAQ.

Le vérificateur constate aussi que, au moment de la vérification sur place, sur les 71 types de fichiers inscrits au plan d'utilisation de 1996, six ont été retirés par le MRQ, lors de la mise à jour de juillet 1998, indépendamment du fait que les extraits de fichiers correspondants aient été reçus ou non.

Un tableau est disponible en annexe au présent rapport pour permettre au lecteur de visualiser, pour les mêmes questionnements, l'état de situation correspondant au plan d'utilisation initial de

[3] La méthode de calcul utilisée par le vérificateur lors de la vérification sur place prend en compte à la fois la provenance ainsi que le type de fichier lui-même. Les chiffres obtenus ne sont pas du même ordre de grandeur que ceux présentés par le MRQ dans le rapport d'activité au 31 mars 2001, puisque ces derniers sont basés uniquement sur le type de fichier.

juillet 1996 et à chacune des trois mises à jour qui ont été approuvées jusqu'à date. Il est à noter que les chiffres présentés à ce tableau peuvent différer de ceux apparaissant en page 14 du rapport d'activité au 31 mars 2001, et ce, parce que certains types de fichiers amènent la réception d'extraits de fichiers en provenance de plus d'un fournisseur et donc, en quelque sorte, une double comptabilisation en terme de types de fichiers. De l'avis du vérificateur, ceci ne fausse toutefois pas l'image d'ensemble de la situation concernant l'obtention réelle des fichiers inscrits au plan d'utilisation, l'impact principal de cette situation étant visible au niveau du plan d'utilisation de juillet 1998 où le chiffre de 67 types de fichiers compilé par le vérificateur passerait à 46 avec la méthode de calcul retenue par le MRQ.

RECOMMANDATION 3

Le MRQ devrait prendre les moyens requis pour n'inscrire au plan d'utilisation que les types de fichiers nécessaires à des projets dont la réalisation est sûre et même imminente.

En outre, le MRQ devrait continuer et même accroître ses efforts visant à éliminer du plan d'utilisation actuel tous les types de fichiers déjà inscrits qui ne répondent pas à des critères très stricts dont celui de nécessité dans un avenir proche.

COMMENTAIRES DU MRQ

« *Le Ministère inscrit au plan d'utilisation les fichiers qu'il considère nécessaires sur un horizon de trois ans et en retire les fichiers pour lesquels aucun besoin n'a été identifié sur une période équivalente. Cette portée concorde avec celle de sa planification stratégique et est usuelle dans l'administration gouvernementale en matière de planification.*

Lors de la mise à jour du plan d'utilisation de l'automne 2000, le Ministère a informé la Commission, dans un document que celle-ci a joint à son avis, de l'effort de rationalisation des activités de lutte contre l'évasion fiscale qui venait d'être entrepris. Il y était entre autres mentionné que plus de 160 projets de lutte avaient vu le jour entre 1996 et 2000 et que le Ministère se concentrait désormais sur une trentaine de dossiers. La mise à jour du plan d'utilisation a permis le retrait de 17 types de fichiers, comme premier résultat de la rationalisation. Cet effort se poursuivra au cours des prochaines mises à jour. »

1.2.4 Le registre public

Le registre public des fichiers obtenus est prévu à l'article 71.0.8 et est tenu à jour par une analyste responsable à la DGI. Le libellé de cet article de la Loi est le suivant : « *le ministre inscrit dans un registre approprié toute communication de fichier de renseignements visée aux*

articles 71.0.2 et 71.0.3 ». Ce registre public apparaît habituellement en tant que tel en annexe au rapport d'activité prévu à l'article 71.0.6 de la Loi, produit au 31 mars de chaque année budgétaire par le MRQ.

Il s'agit, pour l'instant, d'un document complété grâce à un logiciel de traitement de texte (Word). Le vérificateur a été informé que, dans un avenir prochain, des requêtes programmées développées à même le SGF devraient être utilisées pour que le registre des fichiers reçus en vertu du plan d'utilisation soit produit automatiquement par ce système. Deux rapports répondant à l'obligation légale en cause devraient bientôt être disponibles à la suite de l'implantation des nouvelles fonctionnalités du SGF, un sous une forme générale ainsi qu'un autre sous forme détaillée. Celui sous forme générale constituera l'équivalent du registre public actuellement tenu manuellement à la DGI.

CONSTATATIONS

Les entêtes des colonnes du « registre des fichiers reçus en vertu du plan d'utilisation » sont le numéro et le nom du ministère, de l'organisme ou de la municipalité fournisseur de l'information, le numéro et l'identification sommaire des extraits de banques de données reçus ainsi que la période visée dans ceux-ci.

La Loi ne donnant aucune précision sur les qualités d'un registre approprié, le vérificateur ne peut que constater la présence des renseignements fournis par le MRQ.

1.3 Le projet « Profil de richesse »

Le projet « Profil de richesse » vise principalement à détecter les cas à risque en vérifiant la cohérence des déclarations de revenus des ménages, i.e. les individus et leur famille ou autres personnes liées. Les cas recherchés sont ceux qui présentent des signes de sous-déclaration ou de non-production. Ce projet est basé sur la recherche d'indices de richesse. Il vise essentiellement à identifier les ménages qui ont vu leurs actifs croître de façon significativement plus rapide que semblent le permettre les revenus que le MRQ connaît pour ces contribuables et pour les membres de leur ménage. Pour cette clientèle déjà sélectionnée à partir des données fiscales disponibles au MRQ, préalablement à l'obtention des renseignements externes, le but est de tracer un portrait des individus et de leur famille en terme d'acquisition d'actifs par rapport aux revenus du ménage, et ce, au cours des trois dernières années.

Selon les informations obtenues, le MRQ s'est limité, jusqu'à maintenant, à exploiter les fichiers externes uniquement pour des travaux de sélection de dossiers à risque à partir d'indices de richesse ainsi que pour des travaux de recherche et de développement. Ainsi, des accès restreints ont été accordés, surtout au personnel du BLEF, et les résultats des requêtes ont très occasionnellement été transférés aux opérations. De plus, toujours selon les informations obtenues, une journalisation spécifique à ce projet est réalisée de manière à assurer que les personnes utilisant les requêtes préprogrammées d'indices de richesse puissent faire l'objet d'un contrôle *a posteriori* efficace.

Actuellement, même si le projet « profil de richesse » est pleinement opérationnel et qu'il est donc disponible à grande échelle pour l'ensemble du personnel autorisé du MRQ, il n'y aurait qu'une trentaine de vérificateurs qui s'en servent dans tout le Ministère. Plus précisément, d'après le rapport sur les accès autorisés obtenus auprès du personnel du Bureau du mandataire de la centrale de données (BMCD), il y avait seulement 25 utilisateurs des indices de richesse autorisés en date du 31 mars 2001. Selon les informations obtenues, les accès restreints visant les cas de sous-déclarations sont utilisés dans seulement 50 % des régions. Ces régions seraient alimentées en dossiers sur des bases continues. Par contre, pour la recherche de cas de non-production, toutes les régions auraient recours aux requêtes préprogrammées à accès restreints disponibles. Aussi, selon les informations obtenues, en ce qui concerne les projets et activités reliées à la recherche et au développement, la DGCAR et la DGMET se serviraient du projet « profil de richesse » uniquement sur une base *ad hoc*, pour le moment du moins.

CONSTATATION

Selon le vérificateur, l'utilisation actuelle du projet « Profil de richesse » ne représente pas, jusqu'à maintenant, un risque majeur d'utilisation non autorisée en vertu du plan d'utilisation tel qu'approuvé. En effet, les requêtes préprogrammées sont développées par le personnel du BLEF et la programmation de celles-ci demeure sous leur contrôle direct. De plus, l'utilisation de ces requêtes est limitée à un nombre d'utilisateurs potentiels assez restreint et une journalisation spécifique à ce projet est en place permettant un contrôle strict.

RECOMMANDATION 4

Le MRQ devrait maintenir un contrôle serré de l'utilisation du projet « Profil de richesse ».

COMMENTAIRES DU MRQ

> « *Le Ministère exerce déjà un contrôle serré du projet « Profil de richesse », et dans ce sens, appuie cette recommandation.* »

2. LA SÉCURITÉ ET LA PROTECTION DES RENSEIGNEMENTS OBTENUS

Même si, tel que spécifié dans l'introduction du présent rapport, les travaux de vérification réalisés ne constituent aucunement une vérification complète de la sécurité de l'environnement informatique de la centrale de données, le vérificateur a quand même examiné sommairement certains éléments de la sécurité touchant de près les utilisateurs de la centrale.

De plus, une rencontre concernant l'architecture de sécurité de la centrale de données a eu lieu, le 3 avril dernier, avec quelques-uns des principaux responsables ministériels en cette matière. Les

réponses obtenues lors de cette rencontre ainsi qu'au cours de la vérification sur place de même que l'analyse des documents reçus ont mis en lumière certains choix de gestion allant dans le sens de ne pas implanter certaines mesures de sécurité initialement prévues. Dans l'optique de la Commission, la centrale de données devrait bénéficier d'une sécurité optimale en raison du décloisonnement autorisé par le gouvernement du Québec qui fait en sorte que le MRQ détient une quantité exceptionnelle de renseignements personnels particulièrement sensibles concernant tous les citoyens du Québec. Les principaux points de questionnement de la Commission concernent la sécurité des postes de travail, le contrôle des extrants, la sécurité des télécommunications et le cloisonnement de l'environnement de la centrale de données.

Vu le caractère exceptionnel de la situation, la Commission demande au MRQ de réviser l'ensemble des mesures visant à assurer la protection des renseignements externes obtenus et de les bonifier, le cas échéant.

D'autre part, pour mieux informer le lecteur en rapport avec la centrale de données, mentionnons que celle-ci contient, en plus des renseignements externes obtenus en vertu du plan d'utilisation, des renseignements internes déjà disponibles dans le cadre des activités régulières du MRQ ainsi que des renseignements obtenus du gouvernement fédéral. Cette situation entraîne une augmentation importante du nombre de personnes devant disposer d'un accès à la centrale de données. Ceci affecte aussi la complexité du choix des moyens à mettre en place pour assurer la sécurité et la confidentialité des renseignements qui y sont entreposés. Toutefois, les éléments de sécurité examinés pour le présent rapport de vérification s'appliquent, que la source de renseignements impliquée soit de nature externe ou autre. Ceci est vrai sauf pour le point 2.4 du présent rapport touchant la gestion des extrants, laquelle ne concerne que les renseignements externes obtenus en vertu du plan d'utilisation.

2.1 La sécurité des postes de travail des utilisateurs

Le vérificateur a d'abord procédé à la vérification de quelques-uns des éléments de sécurité dont devaient bénéficier les postes de travail « sécurisés » mis à la disposition des utilisateurs de la centrale de données. Rappelons ici qu'il s'agit là uniquement des personnes devant nécessairement accéder aux renseignements externes pour accomplir leur travail et non pas du personnel de support aux utilisateurs qui, lui, n'a accès à ces mêmes renseignements que de façon accessoire.

Les éléments suivants ont fait l'objet de tests auprès de quatre utilisateurs de la DGCAR et de la DGMET : la possibilité de démarrer l'ordinateur à partir d'une disquette de démarrage, la possibilité d'interrompre le démarrage et de démarrer l'appareil en mode sans échec, la vérification obligatoire de l'identité de l'utilisateur grâce au logiciel de gestion du réseau Banyan Vines ainsi que la vérification de la présence d'un écran de veille obligatoire, avec mot de passe correspondant à celui de l'utilisateur du réseau, sans possibilité de le désactiver.

De plus, une prise de connaissance du rôle des gestionnaires dans le processus d'autorisation des accès et de la supervision exercée sur les travaux des utilisateurs a été effectuée, à la même occasion, auprès des chefs d'équipe et chefs de service impliqués.

CONSTATATIONS

Les résultats des tests démontrent que, pour les deux premiers éléments de sécurité prévus, au moins un des quatre postes de travail échantillonnés n'était pas configuré conformément aux attentes exprimées. En outre, il appert que, pour un utilisateur plus connaissant du fonctionnement du logiciel Windows, l'écran de veille obligatoire peut être désactivé, du moins de façon temporaire. Cet écran de veille est toutefois réinstallé automatiquement lors du démarrage subséquent du poste de travail sécurisé.

Même si l'échantillon retenu n'a rien de scientifique, il demeure que les mesures de sécurité, mises en place pour les postes de travail des utilisateurs, n'assurent pas que tous les postes de travail sont sécurisés conformément aux normes prévues. Sans vouloir tirer de conclusions hâtives sur la sécurité des postes de travail et sur les conséquences des manquements observés par rapport à la protection des renseignements externes, le vérificateur ne peut que constater la présence de risques reliés à la configuration des postes de travail dits sécurisés pour les utilisateurs accédant à la centrale. Mentionnons ici que la configuration particulière à ces postes de travail n'est qu'un élément de sécurité parmi d'autres mis en place au niveau de l'accès à la centrale de données.

Quant aux points touchant les gestionnaires, il appert que les chefs d'équipe et chefs de service rencontrés sont bien sensibilisés à l'importance de leur fonction de contrôle lors de l'attribution des profils d'accès à leurs utilisateurs. De plus, ils semblent être en mesure d'exercer une supervision concrète du travail effectué car, normalement, ils demeurent informés des résultats des accès de leurs employés.

Bien entendu, le faible niveau actuel d'appropriation de la centrale de données par les groupes d'utilisateurs de la DGCAR et de la DGMET facilite la tâche des gestionnaires rencontrés et ceux-ci ne semblent pas éprouver une grande difficulté à gérer le risque inhérent aux accès aux renseignements externes par leurs employés. Il est important de mentionner que cette situation est appelée à évoluer dans un avenir prochain.

RECOMMANDATION 5

Le MRQ devrait procéder à une révision des mesures de sécurité qui doivent être implantées, lors de la configuration de chacun des postes de travail des utilisateurs de la centrale de données, puisque celles-ci constituent un des maillons importants de la chaîne de sécurité visant à assurer la protection des renseignements externes obtenus.

Par exemple, lors de l'implantation de Windows 2000 pour l'ensemble des postes de travail du MRQ (projet MIGRE), les postes de travail permettant l'accès à la centrale devraient être configurés de façon conforme aux exigences de protection des renseignements externes obtenus, et ce, dès que possible. En ce sens, il serait sans doute de mise de faire bénéficier, prioritairement,

les utilisateurs de la centrale de données des fonctions de sécurité additionnelles rendues disponibles grâce à cette nouvelle version du logiciel Windows.

COMMENTAIRES DU MRQ

« *Les problèmes liés au démarrage non sécurisé observés par le vérificateur sur un poste de travail ont été corrigés.*

Il faut souligner que les renseignements confidentiels de la Centrale de données sont protégés par un minimum de quatre barrières de sécurité. Dans le domaine des entrepôts de données, ce niveau d'exigence du Ministère est hors du commun. La sécurité des postes de travail n'est que l'une de ces barrières. Pour porter atteinte à la sécurité des renseignements, les autres barrières doivent aussi être franchies. Le caractère sommaire de la vérification en matière de sécurité, telle que l'a qualifiée le vérificateur en introduction au chapitre 2, n'a pas permis de rendre compte de ces considérations.

Par ailleurs, les choix de gestion du Ministère en matière de sécurité sont effectués après une évaluation des risques encourus.

Le Ministère a fait les choix appropriés pour assurer une protection adéquate des renseignements de la Centrale de données, compte tenu des risques envisagés.

La protection des renseignements confidentiels se situe au premier plan des préoccupations du Ministère. Elle constitue l'un des fondements de sa relation de confiance avec les citoyens. Dans ce contexte, le Ministère est constamment à l'écoute de l'évolution des besoins de protection des renseignements et des moyens disponibles pour y arriver. L'évolution des orientations ministérielles en matière de protection des renseignements et de choix de sécurité fait partie intégrante de la planification du Ministère.

Le processus de gestion des postes de travail est en réévaluation. Des boucles de vérification périodiques seront introduites.

De plus, l'une des cibles du projet MIGRE, tel que mentionné par le vérificateur, est la migration de tous les postes de travail du Ministère à Windows 2000. Cette plate-forme bureautique est considérée sur le marché comme plus sécuritaire et plus facile à contrôler que la plate-forme Windows 95 qu'elle remplacera. »

RECOMMANDATION 6

Les gestionnaires d'utilisateurs de la centrale devraient mettre plus d'emphase sur l'étude des besoins spécifiques de chacun de leurs employés en matière d'accès aux renseignements externes de manière à personnaliser encore plus les profils d'accès accordés, et ce, dans l'optique où le nombre d'utilisateurs de la centrale est appelé à augmenter, en particulier à la DGCAR et à la DGMET, et où la nature des finalités poursuivies devrait se diversifier.

Vu que le nombre de gestionnaires exerçant un rôle de surveillance des actions d'employés ayant accès aux renseignements externes devrait augmenter dans un avenir prochain, le MRQ devrait mettre en œuvre un programme de formation destiné à ceux-ci en matière de sécurité et de protection des renseignements personnels.

Les gestionnaires touchés, sans devenir nécessairement des experts en sécurité informatique, seraient alors plus à même de comprendre l'importance des contrôles qu'ils doivent exercer sur le travail de leurs employés accédant à la centrale de données ainsi que l'impact direct de leurs actions pour contrer les problématiques qui sont de leur ressort en matière de protection des renseignements personnels.

COMMENTAIRES DU MRQ

« *La gestion des accès aux renseignements externes est principalement encadrée par la directive interne d'administration " DIA-10 " sur les profils d'accès à la Centrale de données. Celle-ci prévoit déjà qu'il existe un profil d'accès personnalisé et justifié pour chaque utilisateur, parce que chacun est susceptible d'exercer des fonctions distinctes. En outre, les privilèges d'accès aux renseignements externes doivent être autorisés par les sous-ministres adjoints. La directive doit s'appliquer avec la même rigueur, quel que soit le nombre d'utilisateurs.*

D'autres mesures déjà en place vont dans le sens de la recommandation de la Commission. Ainsi, lors de l'autorisation des demandes d'accès à la Centrale de données ou leur renouvellement, il est rappelé aux utilisateurs et à leurs gestionnaires leurs obligations en matière de protection des renseignements externes. Ces obligations incluent la non-divulgation, le respect des finalités et des usages déclarés au plan d'utilisation et dans la demande d'accès, ainsi que le suivi et la destruction des documents et fichiers dérivés.

Le Ministère procède également à des exercices de sensibilisation ad hoc à grande échelle.

Enfin, le Ministère adaptera le contenu de ses programmes de formation en matière de sécurité et de protection des renseignements confidentiels aux

particularités du plan d'utilisation. Par la suite, le Ministère intégrera à sa campagne annuelle de sensibilisation " éthique, confidentialité et sécurité informatique ", un programme de formation spécifique aux gestionnaires responsables de l'utilisation ou de l'exploitation de la Centrale de données.

2.2 La gestion des accès

Une vérification des contrôles mis en place pour assurer la gestion des accès aux renseignements de la centrale de données a aussi été réalisée. Vous trouverez ici un aperçu des principaux contrôles exercés par le MRQ.

Deux groupes distincts interviennent dans les principales opérations relatives à cette gestion. Il s'agit du BMCD, pour l'aspect fonctionnel des demandes, et du responsable ministériel des renseignements externes à la DGI, pour la justification des demandes d'accès en vertu du plan d'utilisation.

Au BMCD, le coordonnateur de la protection des renseignements s'assure de la conformité des demandes d'accès reçues avec les points de contrôle prévus à la directive sur les profils d'utilisateurs de la centrale de données, la DIA-10. Ces points de contrôle visent tout particulièrement l'obtention des signatures requises en fonction de la source des renseignements concernés par la demande d'accès. Rappelons qu'il peut s'agir, soit de renseignements externes obtenus en vertu du plan d'utilisation, soit de renseignements internes déjà disponibles au MRQ ou, encore, de renseignements provenant du gouvernement fédéral. Le coordonnateur veille aussi à implanter les privilèges d'accès aux sources d'information de la centrale. Une autre de ses responsabilités est de s'assurer de la révision des privilèges d'accès selon les principes établis. Le BMCD participe aussi à la reddition de comptes sur les privilèges d'accès accordés.

Ces responsabilités sont exercées tant pour les utilisateurs des renseignements externes que pour les autres personnes agissant à titre de support à ces utilisateurs. Pour bien saisir l'envergure du travail à réaliser, mentionnons que, au 31 mars 2001, on comptait 82 utilisateurs de données parmi lesquels se trouvaient 73 personnes ayant accès aux renseignements externes. De plus, 126 personnes effectuant des activités de soutien disposaient aussi d'un accès autorisé à la centrale de données et 107 d'entre elles avaient accès aux renseignements externes. Les activités de soutien dont il est question ici sont de deux ordres, soit celles de nature purement technique et celles de nature plutôt administrative, telles les fonctions de réception et d'obtention des fichiers ainsi que de préparation des données pour leur exploitation. En résumé, parmi les 208 personnes disposant d'accès autorisés à la centrale de données, 180 avaient accès aux renseignements externes du plan d'utilisation.

Le personnel du BMCD, dont tout particulièrement le coordonnateur de la protection des renseignements, a amélioré et développé, le cas échéant, divers outils pour rencontrer les objectifs de contrôle fixés par le MRQ. Il s'agit principalement des formulaires et annexes utilisés pour les demandes d'accès ainsi que des guides et instructions de travail au regard des accès à la centrale de données.

Le BMCD dispose aussi d'un système appelé le système de gestion de la sécurité ainsi que d'un manuel d'utilisation et de référence afférent. Un calendrier des activités de renouvellement des accès à la centrale de données, complété par un tableau identifiant les utilisateurs pour lesquels le coordonnateur n'a pas obtenu de réponse dans le cadre du processus de renouvellement, est aussi utilisé. Des rapports mensuels et un rapport annuel cumulatif sur les accès accordés sont également produits.

Un autre intervenant majeur, au regard de la gestion des accès, œuvre à la DGI. Il s'agit d'un professionnel disposant d'une vue d'ensemble des travaux de lutte contre l'évasion fiscale et auquel le gestionnaire, responsable des renseignements externes du MRQ, a confié une tâche importante visant à s'assurer que chacun des profils d'accès demandé est justifié en vertu du plan d'utilisation approuvé. En bout de piste, après que les autres mesures prévues en terme de conformité aient été prises, cette personne est appelée à poser une dernière intervention de contrôle avant que les profils d'accès demandés soient implantés réellement et deviennent fonctionnels.

Ce professionnel procède à l'analyse des profils d'accès demandés et à l'examen de la justification les appuyant en se référant principalement au plan d'utilisation. Outre ce plan d'utilisation, son principal outil de travail est constitué des connaissances qu'il a accumulées depuis le début de sa participation aux projets de lutte contre l'évasion fiscale en cours au MRQ. Sa compréhension globale découlant de son implication dans l'étude des documents connexes aux demandes d'accès et des avis de la Commission en général est donc essentielle à la réalisation des objectifs de contrôle qui lui sont confiés.

En cas de doute concernant une demande d'accès en particulier, le professionnel de la DGI a aussi le loisir de recourir au personnel disponible à cet effet, à la Direction générale de la législation et des enquêtes. Ce professionnel a informé le vérificateur qu'il a recours aux services juridiques du MRQ chaque fois qu'il le juge nécessaire.

CONSTATATIONS

L'analyse des informations et documents disponibles au dossier de vérification amène le vérificateur à conclure que le personnel en place et les outils de contrôle utilisés au BMCD assurent, de façon satisfaisante, la réalisation des tâches requises en ce qui concerne les privilèges d'accès des utilisateurs « directs » de la centrale de données.

Toutefois, à la DGI, la réalisation des contrôles visant la justification des demandes d'accès des utilisateurs directs repose, en grande partie, sur les connaissances et les compétences personnelles acquises par le professionnel, auquel on a confié cette responsabilité majeure.

De plus, les mandats actuellement confiés au personnel en place ne comprennent pas de volet visant à s'assurer, tel un mandat de vérification, de la conformité de l'utilisation réelle des renseignements externes avec les accès accordés en vertu du plan d'utilisation.

Finalement, aux yeux du vérificateur, le degré de contrôle réel exercé par le personnel du BMCD et de la DGI est beaucoup plus limité pour le second groupe de personnes disposant de privilèges

d'accès aux renseignements externes. En effet, il est difficile pour les intervenants en contrôle de bien cerner les besoins réels de ces utilisateurs « indirects » et ce fait a un impact notable sur la capacité d'analyse de la justification des privilèges d'accès demandés. Toujours selon le vérificateur, le nombre relativement grand de personnes effectuant des activités de soutien pourrait être dû, en partie, à la problématique habituelle dans les systèmes informatiques qui est d'accorder une priorité absolue au délai de réponse et au service à la clientèle au détriment, bien souvent, de la sécurité et de la protection des renseignements détenus.

Mentionnons toutefois que, lors d'une discussion à ce sujet avec le gestionnaire du BMCD, le vérificateur a pu comprendre que celui-ci était déjà préoccupé par cet état de fait et qu'il avait entrepris de limiter le plus possible les conséquences de ce problème généralement assez répandu dans les milieux informatiques.

RECOMMANDATION 7

Le MRQ devrait prendre les mesures appropriées pour s'assurer de la continuité requise dans l'application des contrôles visant la protection des renseignements personnels et, en particulier, de ceux touchant à la justification des privilèges d'accès demandés par rapport au plan d'utilisation.

Ceci pourrait mener à l'établissement d'une procédure et d'un guide de travail adéquat pour permettre à une personne nouvellement en poste de disposer assez rapidement des compétences et des connaissances requises. Idéalement, une personne devrait être identifiée pour seconder le professionnel de la DGI, actuellement responsable de la réalisation des contrôles en cause, et acquérir ainsi une formation pratique appropriée.

COMMENTAIRES DU MRQ

> « *Les contrôles visant la protection des renseignements externes sont principalement encadrés par les deux directives précitées, DIA-10 et DIA-11. Ces directives prévoient que les responsabilités en matière de protection des renseignements externes sont partagées entre plusieurs intervenants de plusieurs niveaux de gestion, de la sous-ministre aux utilisateurs immédiats des renseignements externes.*
>
> *En particulier, la justification des privilèges d'accès aux renseignements externes est approuvée par le gestionnaire immédiat du demandeur, par son sous-ministre adjoint et par le gestionnaire responsable des renseignements du plan d'utilisation, tous généralement appuyés par des collaborateurs au fait des dossiers.*

Dans l'optique du Ministère, ce partage des responsabilités amène un partage des préoccupations à l'égard des renseignements externes et est un gage de continuité dans l'application des contrôles.

Les directives mentionnées ont été approuvées par le comité directeur ministériel en juin 2000. On peut les considérer en phase de consolidation. Leur mise en oeuvre ne peut que s'améliorer avec le temps, ainsi que le partage d'expertise et la continuité des contrôles qui en découlent. Les efforts de sensibilisation et de formation évoqués dans le contexte de la recommandation 6 de même que la constitution progressive d'une mémoire administrative en matière d'administration des renseignements externes devraient aussi contribuer à l'atteinte de ces objectifs.

Il va de soi que les politiques et directives ministérielles sont implantées dans une perspective de continuité. »

RÉACTION AUX COMMENTAIRES

Les deux directives auxquelles le MRQ fait référence sont très importantes pour assurer un partage des responsabilités entre les différents intervenants du MRQ. Toutefois, compte tenu de la préoccupation exprimée, la Commission considère que ces directives ne permettent pas de répondre aux besoins précis identifiés. En effet, il nous apparaît nécessaire que le MRQ mette en place une procédure particulière accompagnée d'un guide de travail destiné à la personne qui, en bout de piste, est appelée à poser une dernière intervention de contrôle du respect du plan d'utilisation.

RECOMMANDATION 8

Le MRQ devrait confier, à des ressources disposant de l'indépendance et des compétences nécessaires, le mandat de vérifier la conformité de l'utilisation réelle des renseignements externes avec les accès accordés en vertu du plan d'utilisation.

Cette mission devrait être réalisée à titre de contrôle *a posteriori*, en plus de l'analyse systématique des journaux d'accès dont il est question à la section suivante du présent rapport.

COMMENTAIRES DU MRQ

« *Au Ministère, la Direction de la vérification interne et des enquêtes (" DVIE ") dispose des compétences et de l'indépendance nécessaires à la réalisation de ce type de mandat de vérification. Un mandat relatif à la conformité de l'utilisation*

des données externes au plan d'utilisation a été identifié et sera soumis au Comité de vérification du Ministère pour approbation. »

RECOMMANDATION 9

Le MRQ devrait procéder, dès que possible, à l'implantation des mécanismes, informatisés ou non, requis pour compenser le fait qu'un nombre important de personnes œuvrant en support aux opérations des utilisateurs de la centrale doivent disposer de profils d'accès larges leur permettant d'avoir, par le fait même, accès aux données externes elles-mêmes.

Un des mécanismes à envisager serait de réaliser des contrôles *a posteriori*, telle une analyse détaillée des journaux concernant les accès effectués par le personnel de soutien informatique.

COMMENTAIRES DU MRQ

« *La directive interne d'administration DIA-10 sur les profils d'accès à la Centrale de données prévoit que les privilèges d'accès sont révisés annuellement, y compris pour le personnel de support. Cet exercice permet au Ministère de s'assurer que le nombre de personnes disposant d'accès élargis pour des motifs de support est restreint au minimum.*

La gamme de services administratifs et techniques offerts aux utilisateurs d'une centrale de données justifie le nombre de personnes dédiées au support. Le support requiert en effet des efforts importants, qu'il s'agisse de l'alimentation continue en information, de la préparation des informations reçues, du maintien d'une performance adéquate, etc. »

2.3 La journalisation

Le MRQ enregistre et conserve plusieurs éléments d'information essentiels concernant les accès à la centrale de données. Toutefois, même si l'envergure de la vérification en cours ne permet pas de disposer de tous les renseignements nécessaires pour se prononcer, de façon définitive, sur la suffisance et l'intégralité de la journalisation réalisée pour l'ensemble des accès aux données de la centrale de données, le vérificateur a quand même obtenu des informations sur quelques points d'intérêt.

Ainsi, il convient de signaler que, vu l'espace mémoire qu'exigent les divers journaux et les coûts associés à leur conservation pour la période de cinq ans jugée nécessaire, le MRQ conserve uniquement la copie intégrale de chaque requête effectuée à la centrale de données et non pas les résultats de ces mêmes requêtes. Il est quand même possible, par exemple, en cas de doute précis sur les accès d'un employé en particulier, de reprendre le traitement de requêtes à la centrale de

données. Donc, à la condition que les fichiers visés n'aient pas été détruits ou mis à jour depuis le traitement original de la requête en cause, on disposerait à nouveau des résultats de cette requête et ceux-ci pourraient faire l'objet d'une analyse spécifique relativement aux cas douteux.

Signalons que, selon les informations obtenues auprès du BMCD, un processus de journalisation semblable à celui en usage pour les requêtes du projet « indices de richesse » est envisagé de manière à faciliter le contrôle *a posteriori* requis pour les autres types de requêtes.

Mentionnons aussi que les données journalisées n'ont pas encore fait l'objet d'une analyse systémique et régulière. En outre, aucune demande de traitement des journaux n'aurait été initiée depuis le début des opérations de la centrale de données.

Par ailleurs, le MRQ a entrepris l'élaboration d'une directive ministérielle concernant la journalisation des accès aux renseignements confidentiels, la DIA-31. Cette nouvelle directive ministérielle « *vise à encadrer la gestion de la journalisation des accès aux renseignements confidentiels par du personnel du Ministère comme moyen d'en protéger la confidentialité* ». Au moment de la vérification sur place, une deuxième tournée de consultation était en cours.

D'après le texte préliminaire de la DIA-31 dont le vérificateur a obtenu copie, cette directive s'adresse à l'ensemble des activités de traitement informatique du MRQ. Elle ne couvre donc pas les problématiques reliées spécifiquement à l'utilisation des renseignements externes contenus dans la centrale de données.

CONSTATATIONS

Le vérificateur constate que le MRQ ne conserve pas toujours l'information permettant de connaître l'identité des contribuables dont le dossier a été accédé à la centrale de données. De plus, le MRQ ne peut pas être assuré de reconstituer le résultat d'une requête dans le cas où une mise à jour des fichiers requis pour le traitement de celle-ci a été faite depuis ou dans le cas où les fichiers requis pour une réexécution de la requête en cause auraient été détruits.

D'autre part, pour ce qui concerne la centrale de données, le MRQ ne dispose pas encore de programmes informatisés permettant l'analyse systématique et régulière des données journalisées. Le MRQ ne dispose donc pas actuellement des mécanismes qui lui permettraient d'effectuer un contrôle *a posteriori* satisfaisant sur les accès autorisés à la centrale de données.

Cette situation, combinée au fait que le nombre de personnes travaillant en support aux utilisateurs et pouvant accéder aux données externes est relativement élevé, représente un potentiel de non-détection d'une utilisation non autorisée des renseignements externes. De l'avis du vérificateur, ce potentiel existe même en tenant compte des efforts réels du BMCD pour restreindre ce nombre le plus possible.

RECOMMANDATION 10

Le MRQ devrait développer les mécanismes requis pour assurer une journalisation du type de celle effectuée pour les requêtes du projet « indices de richesse ».

De plus, le MRQ devrait faire en sorte que les journaux (logs) des accès à la centrale fassent l'objet, le plus tôt possible, d'une analyse systématique du type de celle réalisée par les employés de la Direction de la vérification interne et des enquêtes et permettant de déceler les cas d'utilisation abusive ou non conforme au plan d'utilisation des renseignements externes obtenus.

Enfin, les gestionnaires d'utilisateurs de la centrale de données devraient, eux aussi, exercer un contrôle *a posteriori* sur les accès effectués par leurs employés, et ce, dès que des rapports d'analyse des journaux de la centrale leur seront rendus disponibles pour ce faire.

COMMENTAIRES DU MRQ

« *Le Ministère journalise déjà les accès à la Centrale de données.*

Dans le cadre des travaux de recherche et développement exigeant de traiter des ensembles de renseignements en vue de cerner des sous-populations à risque, la journalisation permet de connaître, pour chaque personne qui a accédé à la Centrale de données, les requêtes soumises, les populations sur lesquelles ces requêtes portaient et les éléments d'information consultés.

Pour ce qui est des travaux réalisés par le milieu opérationnel lors du traitement des cas à risque du type " profil de richesse ", la journalisation est réalisée dossier par dossier. Le journal informatique contient l'identification de l'employé ayant consulté ou imprimé les renseignements, l'identification du dossier extrait ainsi que le moment où cet accès a été fait.

Pour répondre aux besoins spécifiques de consultation des dossiers par le milieu opérationnel, l'orientation du Ministère est de développer des applications incluant une journalisation au cas par cas du type de celle du projet " profil de richesse ".

Par ailleurs, le Ministère prépare une directive interne d'administration portant sur la journalisation des accès aux renseignements confidentiels. Dans ce cadre, un processus particulier sera mis en place pour analyser les journaux de la Centrale de données. Il est à noter que le Ministère développe et exploite déjà de façon régulière des programmes informatisés qui permettent l'analyse des données journalisées dans ses systèmes opérationnels afin d'identifier les accès non autorisés à des renseignements confidentiels.

Enfin, la directive prévoit qu'à la suite d'un contrôle effectué par la Direction de la vérification interne et des enquêtes, des informations seront mises à la disposition des gestionnaires afin qu'ils s'assurent que leur personnel consulte uniquement les renseignements nécessaires à l'exercice de ses fonctions. »

RECOMMANDATION 11

Le MRQ devrait tenir un registre concernant tout incident ou toute problématique mettant en cause la sécurité de la centrale de données ainsi que la confidentialité et, de façon générale, la protection des renseignements externes de façon à ce que ces cas soient rapportés officiellement et que les informations requises soient accessibles dans les plus courts délais aux hautes autorités du Ministère.

COMMENTAIRES DU MRQ

« *L'architecture cible du plan triennal de gestion de la sécurité informatique du Ministère prévoit une fonction de "SUIVI" qui supporte la "Réponse aux incidents" et la " Gestion des vulnérabilités ". Cette fonction devrait permettre de rencontrer les attentes exprimées dans la recommandation pour ce qui est des incidents en sécurité informatique.*

De plus, La Direction de la vérification interne et des enquêtes, dont le mandat couvre les enquêtes administratives en matière de bris de confidentialité, effectue un suivi rigoureux de tous les manquements à la confidentialité des renseignements, de quelque source qu'ils soient. »

2.4 La gestion des extrants

Les principes de base visant à assurer la confidentialité des renseignements externes, après le moment où ceux-ci ont fait l'objet d'un traitement informatisé à la demande d'un utilisateur autorisé, sont présentés dans la directive ministérielle sur « les documents et fichiers dérivés des renseignements du plan d'utilisation », soit la DIA-11.

Tel qu'abordé au point 1.2.2 du présent rapport, le personnel de la DGI utilise actuellement une application de gestion développée avec MS-Access pour s'assurer de l'étanchéité du processus de destruction des extraits de fichiers reçus des ministères et organismes fournisseurs de données externes prévues au plan d'utilisation.

Quant aux groupes d'utilisateurs vérifiés, à la DGCAR et à la DGMET, ceux-ci ont, selon les informations obtenues lors de la vérification sur place, pris des mesures pour pouvoir identifier en tout temps les demandeurs de leurs régions respectives ainsi que les documents et les extraits de

fichiers qu'ils ont fait parvenir à ceux-ci en réponse à leurs demandes. Un registre d'une forme spécifique à chaque groupe est tenu et est utilisé principalement en vue du processus de destruction annuel, au 31 décembre de chaque année.

De façon à étendre la possibilité d'utiliser des fonctionnalités similaires à celles du système de gestion des extrants actuellement utilisé à la DGI, le MRQ a réalisé, en novembre dernier, une « analyse préliminaire visant à compléter le registre informatisé de gestion des documents dérivés (extrants) ». Un document d'appel d'offre a d'ailleurs été émis récemment et les fournisseurs avaient jusqu'au 23 avril dernier pour présenter leur offre de service correspondante. Il est à noter que l'implantation de la solution retenue est prévue pour le 8 mars 2002.

CONSTATATIONS

Le système de gestion des extrants utilisé à la DGI permet de gérer adéquatement le processus de destruction annuel prévu. Ainsi, les producteurs ou autres utilisateurs de premier niveau de la centrale de données sont formellement avisés de voir à la destruction des documents et fichiers dérivés qui leur ont été transmis par le personnel de la DGI.

Pour le second niveau d'utilisateurs qui sont eux-mêmes les bénéficiaires des résultats des travaux de ces producteurs d'extraits de fichiers, les registres actuellement utilisés semblent habituellement moins structurés et peu mécanisés. Ce fait n'empêche pas nécessairement de rencontrer les attentes normales du processus de destruction. Il suffit sans doute de compenser le manque d'uniformité des processus de contrôle spécifiques, par exemple, par une plus grande implication du personnel en place.

L'appel d'offre visant la mise en œuvre de la DIA-11 devrait permettre au MRQ de disposer de l'outil requis pour « protéger adéquatement les documents et fichiers dérivés des renseignements du plan d'utilisation en s'assurant qu'ils se retrouvent dans un environnement technologique ministériel sécuritaire ».

À ce moment-ci, il convient de rappeler que, dans les mois et les années à venir, « *le MRQ désire augmenter l'utilisation des renseignements inscrits au plan d'utilisation dans le cadre de ses activités de lutte contre l'évasion fiscale* ». La conséquence directe de cette évolution souhaitée par le MRQ est une augmentation importante du nombre de demandeurs d'extrants et d'utilisateurs, ce qui entraîne aussi une augmentation correspondante du risque global de non-respect du processus de destruction établi, affectant ainsi la protection des renseignements externes obtenus.

RECOMMANDATION 12

Le MRQ devrait, en attendant la mise en œuvre de la solution retenue pour la gestion complète des extrants, continuer à fournir les efforts requis pour assurer la confidentialité des documents et fichiers dérivés.

De plus, le MRQ devrait procéder le plus rapidement possible à l'implantation des mesures permettant d'assurer la gestion des extrants requise, et ce, pour tous et chacun des niveaux d'utilisateurs de renseignements externes.

En effet, tant qu'une solution systémique ne sera pas implantée, il y aura un risque accru que, pour toutes sortes de raisons, des renseignements externes devant être détruits soient conservés.

COMMENTAIRES DU MRQ

« *Le Ministère a mis en place un cadre rigoureux de gestion des extrants des fichiers du plan d'utilisation, afin de respecter son engagement de mai 1999 de détruire les fichiers externes et les documents et fichiers qui en sont dérivés à l'expiration du délai de prescription fiscale. La directive DIA-11 sur la gestion des extrants des fichiers du plan d'utilisation, approuvée en juin 2000 par le comité de direction du Ministère, a confirmé les principes en cours d'implantation. Pour appuyer cette mise en œuvre, un registre informatisé des extrants a été rendu disponible aux utilisateurs des renseignements externes. Jusqu'à présent, trois rondes de destruction des extrants ont été complétées.*

Les travaux visant à améliorer la gestion des extrants débuteront en 2002 et s'étendront sur environ 1 an. Le Ministère désire identifier les risques entourant la transmission et la conservation des documents contenant des renseignements externes, évaluer les mécanismes et outils de sécurisation actuellement en place à la lumière des risques identifiés, puis mettre en place l'infrastructure et les processus qui permettront d'améliorer la sécurité, le cas échéant.

Il importe de souligner que l'engagement pris par le Ministère de gérer les extrants d'un système informatique contenant des renseignements confidentiels, comme mesure particulière de protection des renseignements, ne semble pas avoir de précédent au gouvernement du Québec, ni dans les gouvernements similaires. Il n'existe pas d'exemple dont le Ministère puisse s'inspirer. Les façons de faire sont à inventer et ne peuvent s'implanter que progressivement. »

3. LES REVENUS DÉCOULANT DE L'OBTENTION DES FICHIERS EXTERNES

3.1 Le rendement et le système « Portrait ministériel des revenus »

Le présent mandat de vérification comprenait aussi un troisième volet. Il s'agit d'un examen des mécanismes d'information disponibles au MRQ permettant d'identifier et de comptabiliser les revenus découlant de la cueillette des renseignements provenant des fichiers externes, obtenus par le MRQ à la suite de l'adoption du projet de loi n^{o} 32 (1996, chapitre 33) modifiant la Loi.

Pour ce dernier volet, le vérificateur a surtout procédé à une analyse des documents et des informations obtenus lors d'une entrevue avec un professionnel responsable du système appelé PMR.

Succinctement, le système PMR du MRQ est un outil corporatif permettant une reddition de comptes des revenus fiscaux. En fait, le PMR porte sur les revenus comptabilisés et regroupe la totalité des activités du MRQ. Ce système rend donc possible ce que le MRQ appelle la « coloration » des revenus fiscaux du Ministère. Il s'agit là simplement de l'image obtenue à la suite de la répartition des revenus selon le type d'activités ayant mené à leur comptabilisation. On estime à environ 98 % le taux de coloration atteint actuellement. Le système PMR permet donc, entre autres, la mesure des résultats des efforts consacrés à la récupération fiscale.

CONSTATATIONS

Les informations obtenues ont permis de confirmer que le système utilisé actuellement pour effectuer la reddition de compte des revenus fiscaux du MRQ ne permet pas de répondre à l'une des interrogations de base de la Commission. En effet, il a été confirmé que le tableau présentant les résultats de récupération fiscale, selon qu'ils proviennent des activités régulières ou des activités de lutte contre l'évasion fiscale, ne peut, en aucun temps, être assimilé à une reddition de comptes en rapport avec les revenus découlant de l'obtention des fichiers externes.

Les montants d'argent qui apparaissent en annexe au rapport d'activité produit en vertu de l'article 71.0.6 de la Loi, au 31 mars de chaque exercice budgétaire au titre de récupération fiscale dans la colonne « activités de lutte contre l'évasion fiscale », constituent uniquement une reddition de comptes des résultats découlant de l'octroi au MRQ de budgets supplémentaires par le Conseil du trésor, et ce, annuellement depuis 1996.

D'ailleurs, ce fait est corroboré par l'affirmation du MRQ apparaissant à la page 16 du rapport d'activité, identifié précédemment, du 31 mars 2000, à l'effet que « *la récupération fiscale ne peut être directement mesurée à partir de l'utilisation des renseignements externes* ».

RECOMMANDATION 13

Le MRQ devrait procéder aux travaux nécessaires pour se doter d'un système permettant d'évaluer les résultats des activités de lutte contre l'évasion fiscale découlant de l'obtention des fichiers externes, et ce, en termes monétaires.

Bien entendu, tel qu'il ressort des discussions tenues avec des gestionnaires en poste au MRQ, le système en question pourrait commencer par permettre d'identifier les sommes réclamées des individus et entreprises qui étaient inconnues au MRQ avant l'obtention des fichiers de renseignements externes présentés au plan d'utilisation.

Aussi, le MRQ pourrait produire des informations statistiques, portant par exemple sur le nombre de cas de non-production identifiés et sur l'autocotisation qui en découle dans les années ultérieures. Les personnes intéressées disposeraient ainsi d'une base d'évaluation des retombées monétaires, à court et à long terme, découlant de l'obtention de renseignements externes dans le cadre de la lutte contre l'évasion fiscale et, dans un deuxième temps, de la nécessité de l'obtention de ceux-ci.

COMMENTAIRES DU MRQ

« *Tel que l'explique le Ministère dans son rapport d'activité 2000-2001 produit en vertu de l'article 71.0.6 LMR, l'impact de l'exploitation des extraits de banques de données est difficilement mesurable. Répondre à cette attente de la Commission soulève des problèmes de faisabilité importants.*

Comme le note le vérificateur, le Ministère est en mesure de ventiler les résultats de récupération fiscale selon ses domaines d'intervention. En outre, il distingue la récupération fiscale découlant des budgets de lutte contre l'évasion fiscale. Un tel portrait a été joint au rapport d'activité 2000-2001. Cependant, dans plusieurs domaines d'intervention, l'apport des renseignements externes, le cas échéant, est difficile à quantifier.

Le Ministère entreprendra d'ici la fin de l'exercice 2001-2002 une démarche visant à mieux répondre à cette attente de la Commission. »

EN TERMINANT :

La Commission demande au MRQ de lui présenter, dans un délai de trois mois, les mesures qu'il entend prendre en rapport avec les constatations et recommandations formulées ainsi qu'un échéancier de l'application de celles-ci.

La Commission demande également au MRQ de lui faire rapport, dans un délai d'un an à compter du dépôt du présent document, de l'état de la situation en relation avec les constatations et recommandations formulées dans le présent rapport de vérification.

CONCLUSION

La vérification a porté sur le plan d'utilisation des données obtenues à la suite de l'adoption du projet de loi no 32 en juin 1996 ainsi que sur les mesures assurant son respect, sur la sécurité et la protection des renseignements personnels entreposés et utilisés dans la centrale de données et, finalement, sur le rendement découlant de l'obtention des fichiers de renseignements externes dans le cadre de la lutte contre le travail au noir et l'évasion fiscale.

Les constats et recommandations qui constituent les résultats de la vérification permettent de mieux saisir l'envergure et la portée des éléments de contrôle mis en place par le MRQ en vue d'assumer les responsabilités qui lui incombent à titre de détenteur et d'utilisateur des fichiers de renseignements externes.

Tout d'abord, la Commission souligne les efforts consentis par le MRQ pour mettre en place l'organisation du travail et les ressources requises en vue d'assurer l'établissement et le suivi du plan d'utilisation. Les principales constatations portent sur l'amélioration et la mise en place des guides de travail et autres outils nécessaires au personnel assumant des tâches impliquant un rôle de surveillance du respect de ce plan et, ceci, principalement à l'interne.

Quant aux éléments touchant la sécurité et la protection des renseignements, la Commission prend acte de l'intérêt et de la grande sensibilité que les autorités du MRQ accordent à la confidentialité des renseignements recueillis auprès des citoyens, des entreprises, des ministères et des organismes.

Cependant, la Commission est d'avis que le MRQ doit, compte tenu du caractère exceptionnel de l'obtention de nombreux fichiers externes de ministères et d'organismes, s'assurer que la centrale de données dispose de mesures de protection hors du commun. C'est pourquoi, elle invite le MRQ à continuer à être vigilant et proactif dans la gestion des risques informatiques et autres inhérents à la détention, dans la centrale de données, d'une quantité exceptionnelle de

renseignements concernant les Québécois. Elle l'invite aussi à vérifier, de façon exhaustive, l'ensemble de ses mesures visant à assurer la sécurité de la centrale de données.

En ce qui concerne le rendement résultant de la mise en place de la centrale de données, soit les revenus et les recettes découlant de l'obtention des fichiers externes, et en réponse aux demandes répétées du Vérificateur général du Québec ainsi que de la Commission, le MRQ devrait procéder dès que possible à l'étude de faisabilité et aux travaux requis pour apporter des réponses précises et vérifiables à la question de l'impact réel, en termes monétaires, de l'obtention des renseignements provenant de fichiers de ministères et d'organismes gouvernementaux.

COMMENTAIRES DU MRQ

> « *La protection des renseignements confidentiels se situe au premier plan des préoccupations du Ministère. Elle constitue l'un des fondements de sa relation de confiance avec les citoyens. Dans ce contexte, le Ministère est constamment à l'écoute de l'évolution des besoins de protection des renseignements et des moyens disponibles pour y arriver; il demeure vigilant et proactif dans la gestion des mécanismes de sécurité en place afin d'assurer le maximum de protection aux renseignements qu'il détient.* »

En terminant, nous tenons à remercier toutes les personnes du MRQ qui ont collaboré à la réalisation de cette vérification. Leur ouverture d'esprit face à l'évolution requise en termes de protection des renseignements personnels dans le contexte de la mise en place d'un entrepôt, telle la centrale de données, a été grandement appréciée.

ANNEXE MENTIONNÉE À LA PAGE 10

DATE_DÉBUT_PU	DATE_FIN_PU	TYPES DE FICHIERS INSCRITS AU PU (CUMULATIF)	TYPES DE FICHIERS REÇUS	EXTRAITS DE FICHIERS REÇUS (RÉCEPTION INITIALE)	TYPES DE FICHIERS RETIRÉS DU PU (REÇUS OU NON)
01-juil-96	01-juil-98	71	43	170	6
01-juil-98	01-sept-00	67	14	75	17
01-mars-00		2	1	1	
01-sept-00		5	0	0	
TOTAL		**145**	**58**	**246**	**23**
moins RETRAITS DU PU		23	6	12	
SOLDE		122	52	234	

NOTE : Un des 17 types de fichiers retirés du PU de septembre 2000 était constitué de 4 extraits de fichiers. Il s'agit du type de fichier portant le numéro 138. Ces extraits de fichiers n'avaient pas été reçus.

N.B. : Les chiffres présentés dans le présent tableau sont ceux qui étaient disponibles au système SGF en février 2001. À la différence des chiffres diffusés dans le rapport d'activité au 31 mars 2001, le décompte du vérificateur inclut un même type de fichier autant de fois qu'il provient de ministères et organismes différents.