

AVIS

DE LA COMMISSION D'ACCÈS À L'INFORMATION

CONCERNANT

LA REFONTE DES SYSTÈMES PATBQ ET SINPAC

DU

MINISTÈRE DE L'AGRICULTURE, DES PÊCHERIES
ET DE L'ALIMENTATION DU QUÉBEC

DOSSIER 01 08 37
DOSSIER 01 08 38

JUIN 2003

TABLE DES MATIÈRES

INTRODUCTION	1
1. PORTÉE DE L'ÉVALUATION	1
2. DESCRIPTION DES SYSTÈMES.....	2
3. ASSISE LÉGALE.....	3
4. ÉVALUATION DU PROJET.....	3
4.1 L'utilisation d'un NIM	4
4.2 La sécurité des renseignements personnels	6
4.2.1 La politique de confidentialité sur le site Internet.....	6
4.2.2 La convention d'utilisation de la prestation électronique de services	7
4.2.3 L'authentification du requérant lors de transactions par Internet	8
4.2.4 L'acheminement d'un mot de passe dans le cas d'oubli.....	9
4.2.5 La sécurité des transactions.....	9
4.2.6 L'intégrité et la journalisation.....	11
4.2.7 La sécurité des échanges de l'information	11
4.2.8 Conservation des renseignements personnels	13
CONCLUSION	14

INTRODUCTION

Le ministère de l'Agriculture, des Pêcheries et de l'Alimentation du Québec (MAPAQ) procède actuellement à la refonte du système Programme d'analyse des troupeaux de boucherie du Québec (PATBQ) et du système Programme d'aide aux entreprises agroalimentaires (SINPAC). Les responsables du MAPAQ évoquent que l'architecture de ces systèmes est basée sur des concepts de réalisation datant du début des années 1980 et qu'ils sont appuyés sur une technologie désuète. De plus, ils soulignent l'évolution importante des pratiques zootechniques et agroalimentaires, la volonté du MAPAQ à poursuivre les orientations gouvernementales en regard de l'implantation future du système gouvernemental GIRES et de l'utilisation de l'inforoute concernant l'amélioration de ses relations avec les citoyens.

Afin de s'assurer que ce projet est conforme à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès), les responsables du MAPAQ demandent un avis de la Commission d'accès à l'information (Commission) en regard des données véhiculées et échangées par ce système et, plus particulièrement, dans le contexte où les producteurs, les pêcheurs et les vétérinaires auront la possibilité de consulter et de mettre à jour, par Internet, les données qui les concernent. La prestation électronique de services développée par le MAPAQ sera aussi destinée aux syndicats de gestion et les clubs agro-environnementaux, les usines de transformation, les universités et les corporations municipales.

Il faut souligner que la Commission émet un avis pour les deux systèmes (PATBQ et SINPAC) puisque l'approche technologique et le fonctionnement même des systèmes se recoupent en terme de similitude.

1. PORTÉE DE L'ÉVALUATION

L'évaluation repose principalement sur les informations contenues dans les documents qui nous furent transmis par le MAPAQ et sur les réponses aux questions spécifiques transmises aux responsables désignés du MAPAQ.

L'analyse a porté principalement sur la conformité du projet, au stade de l'analyse préliminaire et de l'architecture de systèmes, aux principes de protection des renseignements personnels. Les mesures de sécurité ont été abordées de façon non exhaustive, la technologie utilisée n'a pas fait l'objet d'une évaluation technique et la sécurité en place n'a pas fait l'objet de corroboration. La nécessité des renseignements colligés n'a pas été analysée, non plus les communications de renseignements personnels prévues à partir des systèmes sous étude.

2. DESCRIPTION DES SYSTÈMES

Le système PATBQ refondu doit offrir toutes les facilités nécessaires pour supporter les nouveaux défis en matière de pratiques zootechniques dans le domaine du bœuf, lesquelles sont actuellement utilisées par l'industrie et dont la clientèle est composée des producteurs de bovins, des superviseurs et des propriétaires d'abattoirs. Les principaux objectifs du système sont, d'une part, d'améliorer la productivité, l'efficacité et la rentabilité des troupeaux de bovins de boucherie du Québec et, d'autre part, d'offrir un instrument souple, moderne et unique de sélection et d'évaluation génétique de bovins de boucherie dans les Amériques. Le système PATBQ transmet des informations à une entreprise ontarienne « Beef Improvement Ontario » qui effectue des calculs de performance du potentiel génétique et retourne l'information sur les écarts prévus. Le système transmet également des informations au Centre d'insémination artificielle du Québec afin d'obtenir des suggestions d'accouplement. Enfin, le système échangera des informations avec le système intégré de gestion de la clientèle du MAPAQ.

Les employés du MAPAQ utilisateurs du système PATBQ sont situés au central à la Direction des services technologiques et en région (25 sites). Grâce à la technologie Web, il est prévu que le nouveau système deviendra directement accessible à tous les producteurs de bovins du Québec. D'autres intervenants sont également considérés, les superviseurs, la Régie de l'assurance agricole du Québec, la Fédération des producteurs de bovins du Québec, les fournisseurs de services externes et les propriétaires d'abattoirs.

Quant au système SINPAC, celui-ci gère l'information d'une grande partie de la clientèle du MAPAQ, notamment les producteurs agricoles, les pêcheurs et les vétérinaires. De ce fait, plusieurs systèmes s'alimentent d'informations provenant de SINPAC. De plus, le système actuel génère des transactions monétaires qui sont traitées par le système gouvernemental SYGBEC.

Le système SINPAC est le principal support informatique du Service des subventions et de la Direction générale des affaires régionales (DGAR) concernant les activités associées à l'administration des principaux programmes d'aide aux entreprises agricoles.

Le personnel du Service de soutien à la gestion de programmes constitue les principaux utilisateurs du système au central. Les utilisateurs se composent du personnel de saisie, des gestionnaires et du pilote de système. En région, les utilisateurs se répartissent dans une soixantaine de sites (bureaux régionaux et locaux). C'est en région que sont saisies les informations de la fiche d'enregistrement ainsi que certaines transactions concernant les programmes de subvention. Les utilisateurs sont le personnel de secrétariat, des agronomes et des conseillers agricoles.

Le système refondu utilisera le potentiel offert par les technologies Web pour transmettre de l'information en région.

Par ailleurs, il est également envisagé que les producteurs agricoles (environ 33 000) puissent utiliser l'Internet pour consulter et mettre à jour leurs dossiers.

Le système SINPAC gère également le programme de remboursement de frais de vétérinaires de la Direction de l'épidémiologie et de la santé animale (DESA). À cette fin, les cliniques vétérinaires qui transmettent actuellement leurs relevés d'honoraires par la poste deviendront des usagers puisqu'ils pourront les transmettre par Internet et éventuellement consulter leurs dossiers. Un projet pilote concernant la transmission électronique des relevés d'honoraires a confirmé la faisabilité de la transmission par Internet. Actuellement, il y a environ 400 vétérinaires qui participent à ce programme. Les vétérinaires auront de plus accès à l'information relative à l'atteinte du quota d'un producteur pour les services assurés.

La refonte des systèmes PATBQ et SINPAC permettra au plan technologique de remplacer une technologie dépassée et coûteuse à entretenir. De plus, l'architecture technologique actuelle s'avère instable, le maintien de l'intégrité des données est difficile et les fonctionnalités habituellement offertes par un système de gestion de base de données (SGBD) ne sont pas supportées. Ainsi, le manque d'automatismes de suivi de la clientèle, la lourdeur d'utilisation des systèmes actuels, leur fragilité technologique et la vulnérabilité des mécanismes de sécurité sont les principales raisons qui empêchent de les rendre disponibles directement auprès de la clientèle.

3. ASSISE LÉGALE

La *Loi sur le ministère de l'Agriculture, des Pêcheries et de l'Alimentation* (L.R.Q., c. M-14) édicte que le ministre est chargé de la direction et de l'administration du ministère. Les systèmes PATBQ et SINPAC constituent des outils que le ministre s'est donné afin de répondre à cette obligation en matière d'administration et qui lui permettent d'exercer les fonctions, pouvoirs et devoirs qui lui sont dévolus par la loi du MAPAQ.

4. ÉVALUATION DU PROJET

Les systèmes refondus du MAPAQ utiliseront un numéro d'identification ministérielle unique appelé NIM en regard de la gestion des dossiers de la clientèle. L'utilisation de ce nouvel identifiant fera l'objet d'une évaluation.

En plus des améliorations technologiques, la refonte des systèmes vise la mise en place d'une prestation électronique de services (PES) par le recours aux technologies Web pour le transfert d'informations aux bureaux régionaux, à la clientèle et à des organismes externes. Cette nouvelle avenue nécessite une évaluation en regard de la protection des renseignements personnels, plus particulièrement concernant l'authentification à distance de la clientèle du MAPAQ.

4.1 L'utilisation d'un NIM

Le NIM est conservé dans une base de données indépendante et est produit par le système de génération et de contrôle des NIM. Ce système retourne un numéro unique pour une demande d'inscription d'un client et assure l'attribution d'un seul NIM pour un numéro d'entreprise (NEQ) ou un numéro d'assurance sociale donné.

Les responsables du MAPAQ établissent ainsi la nécessité d'utiliser un NIM :

« Ce numéro unique vise à simplifier la vie aux clients qui veulent transiger avec le MAPAQ en leur évitant d'avoir à mémoriser plusieurs identifiants. »

Présentement, le MAPAQ identifie sa clientèle dans chacun des programmes. Il n'existe pas d'application permettant de gérer les clients du MAPAQ pour l'ensemble des programmes auxquels ils participent. Aussi, le NIM aura-t-il pour mission de centraliser et de normaliser l'attribution d'un numéro d'identification unique à toute la clientèle du MAPAQ. Des tables de correspondance permettront de lier le NIM aux identifiants actuels (CP12, NEQ, NAS...) requis par les systèmes opérationnels.

La Commission comprend que des considérations de cohérence amènent le MAPAQ à envisager la consolidation de son fichier de clientèle. La Commission rappelle toutefois que l'identification unifiée de la clientèle ne doit pas avoir pour effet de réduire la protection des renseignements personnels détenus par le MAPAQ.

À cet égard, les responsables du MAPAQ mentionnent :

« L'introduction du NIM vise à accroître la protection des renseignements personnels. En effet, ce numéro d'identification est purement séquentiel et, contrairement au CP12, il ne comporte rien de personnel concernant le producteur. »

Aussi, la nécessité de la cueillette devra continuer de s'apprécier par programme, de même que les accès et les utilisations des renseignements devront respecter la finalité prévue au moment de la cueillette et, enfin, les délais de conservation devront demeurer proportionnels aux besoins d'application du programme.

Les responsables du MAPAQ mentionnent à cet égard :

« Il faut comprendre que l'utilisation d'un système pour générer un NIM ne vise pas à rassembler dans un système unique l'ensemble des systèmes du ministère. En effet, chaque système garde son indépendance, sauf qu'un client commun à plusieurs systèmes sera identifié de façon unique dans les différents systèmes. Donc, tel que souhaité par la CAI, la nécessité de la cueillette continuera de s'apprécier par programme. De

même, les accès et les utilisations respecteront la finalité prévue au moment de la cueillette. Aussi, les délais de conservation demeureront proportionnels et spécifiques aux besoins d'application du programme. Finalement, il importe de rappeler que chaque système a ses propres règles de sécurité quant à l'aspect applicatif. Ainsi, une permission accordée à un individu pour une application n'a aucune influence sur les restrictions fixées à l'individu dans une autre application.

À titre d'exemple d'appréciation de la sécurité de la cueillette par programme pour PATBQ, les renseignements personnels recueillis auprès des producteurs de bovins sont le nom, l'adresse, le numéro de téléphone et l'adresse de courriel. Les autres données recueillies concernent la description des animaux en vue d'une évaluation génétique de ceux-ci. »

La Commission attire l'attention du MAPAQ sur le caractère confidentiel du NIM lorsque celui-ci permet d'identifier une personne. Le MAPAQ se doit de prendre les mesures de sécurité adéquates pour préserver le caractère confidentiel de cet identifiant. Les documents déposés prévoient l'utilisation d'un fichier témoin « cookie » contenant le NIM lors des accès à distance. La Commission demande au MAPAQ de revoir cette façon de faire et de prendre garde de ne pas, dans la prestation de services à distance, générer un fichier témoin « cookie » contenant le NIM ou d'autres renseignements personnels. Une telle pratique facilite, d'une part, l'usurpation d'identité et pourrait contribuer à la divulgation de renseignements personnels (par exemple, lorsqu'un poste est utilisé par plusieurs individus).

Les responsables du MAPAQ mentionnent en regard de l'utilisation des fichiers témoins « cookies » :

« [...], le MAPAQ avait effectivement amendé, il y a plusieurs mois, sa façon de faire pour éviter de générer un cookie contenant le NIM ou des renseignements personnels. Donc, les cookies actuels ne contiennent aucun renseignement personnel.

Un premier cookie facilite le travail de l'utilisateur en lui évitant de s'identifier à répétition au cours d'une même session de travail. La durée de vie de ce cookie correspond à la session de travail. Lorsque l'utilisateur met fin à sa session de travail, le cookie disparaît de la mémoire vive de l'ordinateur.

Le deuxième cookie demeure sur le poste de l'utilisateur et permet de faciliter son identification lors d'une prochaine session de travail. Mais ce dernier cookie contient uniquement un numéro sans aucune signification. »

Par conséquent, dans le contexte des systèmes du MAPAQ et compte tenu que chaque système garde son indépendance, que la cueillette continue de s'apprécier par programme et que le NIM n'est plus intégré dans un fichier témoin « cookie », la Commission n'a pas objection à l'utilisation du NIM.

4.2 La sécurité des renseignements personnels

Les responsables du MAPAQ préconisent l'utilisation du Web dans le cadre de la refonte des systèmes PATBQ et SINPAC, ils soulignent à cet égard :

« Le respect des orientations gouvernementales privilégiant l'utilisation du Web pour rejoindre la clientèle combiné au potentiel de cette technologie pour échanger de l'information avec les régions favorisent nettement son utilisation dans le cadre de ce projet. »

Les règles du jeu dans un contexte d'Internet sont fortement différentes si nous considérons : l'échelle mondiale de la publicité donnée à une information, la facilité et le faible coût des informations, la captation et la réutilisation très simples des informations diffusées et les traces laissées par les navigations tant sur les serveurs consultés que chez les fournisseurs d'accès, lesquelles sont autant de réalités inhérentes à la technologie qui peuvent porter atteinte à la protection des renseignements personnels si leur diffusion n'est pas bien encadrée. Le mode de diffusion qu'est l'Internet présente des risques qui exigent qu'on adopte les garanties suivantes avant d'y faire circuler des renseignements personnels.

4.2.1 La politique de confidentialité sur le site Internet

La Commission demande au MAPAQ de prévoir rendre accessible, dans sa page d'accueil du site Internet, une « Politique de confidentialité » concernant l'utilisation des informations recueillies lors de l'accès au site par les clients. La Politique devra énoncer clairement les mécanismes et les procédés automatiques concernant :

- les mesures de sécurité assurant la confidentialité des renseignements personnels fournis par une personne requérante, notamment aux fins de paiement, de facturation et de transmission de documents demandés, de même que les finalités, les utilisations, les catégories de personnes y ayant accès, les modalités de conservation et droits d'accès et de rectification;
- l'utilisation de fichiers témoins « cookies » ou toute autre forme de collecte d'informations concernant la visite de l'internaute recueillie à son insu;
- les communications d'informations transmises automatiquement entre les serveurs;
- les liens vers d'autres sites.

Concernant la diffusion d'une politique des services en ligne, les responsables du MAPAQ soulignent :

« Une réflexion est actuellement en cours au MAPAQ pour produire une « Politique pour les services en ligne » concernant les points énoncés par la CAI. On trouvera dans cette politique générale rédigée en français, toutes les préoccupations d'un utilisateur relatives à notre site Internet. Ainsi, il aura des explications sur les services en ligne, les conditions d'utilisation, la politique de confidentialité et les mesures de sécurité.

De plus, dans chacun des systèmes offerts en prestation électronique, on indiquera les spécificités qui lui sont propres. Aussi, concernant la langue, un client ayant des difficultés avec le français pourra s'adresser à l'unité administrative concernée pour obtenir une traduction. »

4.2.2 La convention d'utilisation de la prestation électronique de services

La Commission comprend qu'une convention est en rédaction. Le MAPAQ devrait fixer et faire accepter des conditions d'utilisation qui encadreront la prestation électronique de services avec ses clients. Par conséquent, la Commission demande au MAPAQ de mettre en œuvre toutes les mesures de sécurité lui permettant d'assumer la plus grande part de responsabilités au regard d'une transaction impliquant des renseignements personnels. La Commission lui demande ensuite de fixer les modalités de la convention à intervenir entre les parties.

Par cette convention, il est impératif que le client soit informé des risques encourus, des mesures qu'il est responsable de mettre en œuvre et de la responsabilité résiduelle du MAPAQ en regard de la protection des renseignements personnels impliqués dans toute transaction.

Cette convention pourrait être jointe à toute entente sur l'échange électronique de données signée avec les unions de producteurs et autres.

Il est usuel, particulièrement dans les transactions commerciales, de voir un tel partage des risques et les conséquences, le plus souvent financières, deviennent alors acceptables pour les parties. En matière de protection des renseignements personnels, l'organisme public porte seul la responsabilité des renseignements personnels qu'il recueille, détient, utilise et communique. De plus, on devra considérer que la réparation des conséquences potentielles d'un bris de confidentialité est souvent plus complexe que le règlement d'un litige financier.

4.2.3 L'authentification du requérant lors de transactions par Internet

L'entrée en vigueur de la *Loi concernant le cadre juridique des technologies de l'information* de même que les modifications apportées à la Loi sur l'accès consacrent la possibilité de fournir un service à distance, sans toutefois réduire les exigences en matière d'identification et de signature.

Les technologies Web et l'Internet sont certes une voie privilégiée pour faciliter la communication entre le MAPAQ et sa clientèle. La Commission reconnaît que le MAPAQ fournira une prestation de services à distance, notamment auprès des producteurs; à cet égard, des mesures devront être mises en place pour identifier l'interlocuteur adéquatement lors de transactions par Internet.

La documentation de l'analyse préliminaire et d'architecture indique que le MAPAQ prévoit comme moyen d'authentification l'utilisation d'un identifiant et d'un mot de passe. L'article 38 de la *Loi concernant le cadre juridique des technologies de l'information* édicte :

38. Le lien entre une personne et un document technologique, ou le lien entre un tel document et une association, une société ou l'État, peut être établi par tout procédé ou par une combinaison de moyens dans la mesure où ceux-ci permettent :

1° de confirmer l'identité de la personne qui effectue la communication ou l'identification de l'association, de la société ou de l'État et, le cas échéant, de sa localisation, ainsi que la confirmation de leur lien avec le document;

2° d'identifier le document et, au besoin, sa provenance et sa destination à un moment déterminé. »

Lorsqu'il est question de renseignements personnels, la Commission croit que l'identification de la personne à distance doit être effectuée de façon impérative. Le MAPAQ ne pourrait communiquer des renseignements personnels considérés confidentiels à moins de s'assurer que cette communication soit destinée à la personne concernée.

Le processus d'authentification utilisé par le MAPAQ lors de transactions par Internet est le suivant :

« [...] Quant au processus d'authentification du ministère, on doit savoir que les clients recevront par la poste leur numéro d'authentification ministériel (NIM) et un formulaire les invitant à utiliser la prestation électronique de service (PES). Le client intéressé devra signer et retourner ce formulaire de demande de mot de passe à son contact au ministère. Ce dernier entrera dans le système pour demander la génération d'un mot de passe temporaire qui sera envoyé directement du système vers le client par

courriel. Aucune personne intermédiaire ne voit ce mot de passe, même pas le contact ministériel. Avant d'accéder au système, le client est obligé de changer le mot de passe temporaire par un mot de passe à son choix, [...].

En ce qui concerne la confection du mot de passe par le client, des règles strictes doivent être respectées, autrement le mot de passe est rejeté. Par exemple, un client ne peut réutiliser l'un de ses cinq derniers mots de passe. Son mot de passe doit contenir de 8 à 30 caractères et être composé d'un mélange de chiffres et de lettres sans répéter successivement plus de deux fois le même caractère. »

Dans le contexte des risques associés aux systèmes mis en place par le MAPAQ, la Commission considère qu'un tel modèle de prestation électronique de services est suffisant pour offrir les services en ligne sécurisés. Par ailleurs, la Commission appuie le MAPAQ dans son désir de poursuivre ses efforts dans le renforcement du processus d'authentification mis en place.

4.2.4 L'acheminement d'un mot de passe dans le cas d'oubli

La Commission note que les documents fournis prévoient que l'attribution d'un mot de passe est retransmis en cas d'oubli du mot de passe.

Les responsables du MAPAQ mentionnent :

« [...] Ainsi, dans cette dernière situation, après avoir cliqué sur une case « J'ai oublié mon mot de passe », le client voit apparaître la question qu'il avait choisie. S'il répond correctement à la question, le système lui rappelle son mot de passe. Dans le cas contraire, il doit contacter son conseiller afin que celui-ci fasse une nouvelle demande de mot de passe temporaire qui devra être modifié avant la première utilisation.»

La Commission considère que le mécanisme de rappel du mot de passe décrit par le MAPAQ présente un risque de divulgation du mot de passe et d'usurpation d'identité.

4.2.5 La sécurité des transactions

Le développement d'une interface conviviale pour les utilisateurs et la sécurité des transactions sont des éléments d'importance dans un environnement Web. Le MAPAQ souligne à ce sujet :

« [...], il faut ajouter les facilités de saisie en direct en mode Web directement dans le nouveau système [...]. Cette approche implique cependant qu'un bon nombre de clients externes voudront bien saisir eux-mêmes leurs données. [...]. Nous retrouvons donc ici l'importance de

développer une interface utilisateur qui doit être très simple d'utilisation pour les clients afin de favoriser la saisie de données le plus près possible de la source. »

À cet égard, la Commission appuie le MAPAQ dans sa démarche de porter une attention particulière au développement de fonctions simples et ergonomiques sur son site pour que sa clientèle, généralement inexpérimentée sur le Web, puisse aisément mettre en œuvre les mesures qui lui incombent.

Par ailleurs, la Commission met en garde le MAPAQ sur les vulnérabilités particulières amenées par l'utilisation des outils Web et de l'Internet. Ce mode de communication a ceci de distinctif, l'organisme qui offre le service ne peut, à lui seul, garantir la sécurité et la confidentialité de la transaction.

En effet, ces technologies présentent de façon inhérente des failles sur le plan de la sécurité et les risques se doivent obligatoirement d'être partagés entre le MAPAQ et son client. Le MAPAQ peut sécuriser de façon robuste son infrastructure; toutefois, l'utilisation d'un réseau public, comme l'Internet et d'un fureteur Web, exige que le client soit invité à prendre des précautions pour assurer la sécurité et la confidentialité de la transaction. Plusieurs exemples illustrent les précautions à prendre :

- le client doit pouvoir effacer la mémoire cache à la fin de chaque session puisque certains renseignements personnels reçus ou transmis durant la session se trouvent sur le poste qu'il utilise;
- il doit s'assurer de fermer la session personnalisée adéquatement;
- il doit s'assurer que le sceau de sécurité est présent lors de la transmission de renseignements personnels;
- il ne doit pas utiliser le courrier électronique pour communiquer des renseignements personnels à moins de chiffrer l'information;
- l'utilisation d'un pare-feu personnel est souvent recommandée par les institutions financières offrant des services en ligne; etc.

De tels éléments de sécurité des transactions devraient faire partie de la convention d'utilisation.

Les responsables du MAPAQ soulignent :

« Le MAPAQ va effectivement rappeler à l'utilisateur les précautions nécessaires pour assurer la sécurité et la confidentialité de ses transactions. Avec le formulaire de demande d'accès aux services en prestation électronique, le client recevra les mises en garde propres à maintenir un fonctionnement sécuritaire et qui l'éclaireront sur les responsabilités du MAPAQ et les siennes. »

4.2.6 L'intégrité et la journalisation

Afin que l'article 38 de la *Loi concernant le cadre juridique des technologies de l'information* puisse trouver son application, le MAPAQ devra s'assurer que les transactions effectuées par le client à la suite de la confirmation de son identité seront journalisées de sorte qu'un lien puisse être établi entre ce client et les actes posés dans son dossier.

Les responsables du MAPAQ mentionnent à cet égard :

« Il est déjà prévu de journaliser toutes les transactions effectuées par le client. Ainsi, toute mise à jour est journalisée. Semblablement, les consultations d'informations sensibles sont journalisées, sauf pour quelques personnes comme le gestionnaire des bases de données, le pilote de système et les analystes qui entretiennent le système. La documentation de ces exceptions pour la consultation est en cours et un engagement signé sera exigé de la part des personnes visées. »

Afin de permettre aux journaux de représenter le lien entre une personne et une action et de préserver l'intégrité de ce lien, des mesures particulières devront être prises par le MAPAQ afin de maintenir l'intégrité des journaux et des autres documents pouvant être admis en preuve.

Les responsables du MAPAQ expliquent les mesures prises à ce sujet :

« Pour préserver l'intégrité des journaux faisant le lien entre une personne et une action, nous limitons l'accès à ces journaux en permettant l'écriture uniquement par les applications de façon automatique à chaque fois qu'une modification est effectuée par un intervenant dans une banque. Chaque jour une copie des journaux est faite sur un support magnétique et archivée dans une voûte. En plus de ce mécanisme de journalisation, le logiciel de gestion des bases de données ORACLE procède à la journalisation de toutes les transactions dans ses propres journaux. Ces derniers font l'objet d'une copie de sécurité journalière également remise en voûte à l'extérieur des locaux. Quant aux serveurs de bases de données eux-mêmes, ils sont dans une salle barrée accessible à quelques informaticiens seulement. »

4.2.7 La sécurité des échanges de l'information

La Commission comprend que le MAPAQ entend intégrer les échanges d'informations dans la refonte des systèmes et dotera son infrastructure technologique des mécanismes de sécurité nécessaires à la protection des renseignements personnels qui y seront véhiculés. Ainsi, le MAPAQ s'engage à se doter d'une robuste protection qui empêchera

les intrusions dans la banque de données en zone de diffusion par l'instauration de bastions, de contrôles des virus et de mécanismes de détection des intrusions. Par conséquent, les mesures de sécurité qui encadreront les échanges de renseignements personnels devront assurer l'intégrité et la confidentialité des informations par le chiffrement lorsque celles-ci seront transmises sur le réseau Internet, de même que sur tout réseau partagé. À cet égard, la Commission comprend que le MAPAQ s'engage notamment à avoir recours au mode de sécurité SSL pour ses transactions interactives.

D'ailleurs, les responsables du MAPAQ mentionnent :

« Ainsi, les échanges interactifs avec les clients sont sécurisés avec le protocole SSL et toute l'information est encryptée. Dans le cas des rapports, ceux-ci sont encryptés avec WINZIP sur les serveurs de production et le transfert est sécurisé avec le mode SSL. Quant aux banques de données, on notera que le NIM n'est pas une clé d'accès. Nous utilisons plutôt un numéro interne à la banque qui n'est pas connu à l'extérieur. »

Par ailleurs, la Commission comprend que le MAPAQ exercera un contrôle rigoureux en regard des privilèges d'accès relatifs aux renseignements personnels contenus dans la banque de données, et ce, autant de l'interne que de l'externe. La mise en place des mesures de sécurité doit permettre de s'assurer, qu'à l'interne, seules les applications pourront modifier la banque de données; ainsi, même les informaticiens ne pourraient altérer les données.

Les responsables du MAPAQ mentionnent :

« Actuellement, nous anticipons que les administrateurs de base de données (DBA) soient les seules personnes capables de modifier les données sans passer par les applications. Toutefois, ses requêtes de modification seront journalisées. »

En matière de communication de renseignements personnels, les documents déposés indiquent que le MAPAQ rendra disponibles aux vétérinaires des renseignements relatifs à l'utilisation par les producteurs de services vétérinaires subventionnés. Par ailleurs, les documents techniques indiquent qu'on entend contrôler l'accès des vétérinaires à ces données par région. Nous rappelons au MAPAQ que les renseignements personnels concernant un producteur ne pourront être communiqués à un tiers sans le consentement du producteur.

Les responsables du MAPAQ apportent les précisions suivantes :

« Les seules informations accessibles aux vétérinaires seront le montant résiduel disponible pour une intervention vétérinaire chez le producteur et le statut de celui-ci, à savoir s'il est radié ou non du programme d'aide de soins vétérinaires. »

Toutefois, on notera, par rapport aux documents déjà présentés à la CAI, une évolution dans les besoins d'accès d'un vétérinaire. En effet, au lieu de limiter par région, les accès d'un vétérinaire seront limités aux producteurs dont il connaît le NIM. Ceci est nécessaire pour lui permettre de vérifier les informations précédemment mentionnées avant d'effectuer une visite chez un producteur peu importe la région où il se situe. »

Ainsi, la Commission comprend que le MAPAQ limitera les accès d'un vétérinaire aux seules données nécessaires.

4.2.8 Conservation des renseignements personnels

Les documents déposés indiquent que tous les renseignements personnels colligés par le MAPAQ sont conservés et qu'un statut d'archivage dont les règles seront définies est appliqué le cas échéant. Rappelons que la conservation des renseignements personnels doit être soumise à un calendrier de conservation et que l'article 73 de la Loi sur l'accès établit qu'un renseignement devrait être détruit lorsqu'il n'est plus utile.

73. Lorsque l'objet pour lequel un renseignement nominatif a été recueilli est accompli, l'organisme public doit le détruire, sous réserve de la Loi sur les archives (chapitre A-21.1).

La Commission demande donc au MAPAQ d'adopter un calendrier de conservation et de déterminer les délais de conservation applicables aux renseignements détenus.

Les responsables du MAPAQ mentionnent à cet égard :

« Le MAPAQ compte adopter un calendrier de conservation spécifique à chaque application et déterminer les délais de conservation applicables aux renseignements détenus. Ce travail sera fait au moment de la conception de la solution d'archivage prévue vers avril 2004. »

CONCLUSION

L'analyse a porté principalement sur la conformité du projet, au stade de l'analyse préliminaire et de l'architecture de systèmes, aux principes de protection des renseignements personnels. Toutefois, la nécessité des renseignements colligés n'a pas été analysée, non plus les communications de renseignements personnels prévues à partir des systèmes sous étude.

Dans le cadre de la refonte du système PATBQ et du système SINPAC, les responsables du MAPAQ ont fait ressortir le besoin d'accroître l'efficacité des systèmes et de favoriser l'utilisation de l'infrastructure afin d'améliorer ses relations avec les citoyens.

Les pratiques décrites par le MAPAQ illustrent sa volonté de mettre en place des mesures de protection des renseignements personnels, et ce, à l'intérieur d'une infrastructure technologique sécuritaire.

La Commission comprend que la nécessité de la cueillette de l'information continuera de s'apprécier par programme, de même que les accès et les utilisations des renseignements respecteront la finalité prévue au moment de la cueillette.

La Commission prend acte de l'engagement du MAPAQ à produire une « Politique pour les services en ligne ».

La Commission demande au MAPAQ de poursuivre ses efforts dans le renforcement de son processus d'authentification pour les services en ligne.

Enfin, la Commission prend acte que le MAPAQ compte adopter un calendrier de conservation et déterminer les délais de conservation applicables aux renseignements détenus.

Par conséquent, la Commission émet un avis favorable en regard du présent dossier.