AVIS CONCERNANT

LE CADRE GLOBAL DE GESTION

SUR LA SÉCURITÉ DES ACTIFS INFORMATIONNELS

DU RÉSEAU DE LA SANTÉ ET DES SERVICES SOCIAUX

Dossier 01 11 11

DÉCEMBRE 2001

Le 6 juin dernier, le ministère de la Santé et des Services sociaux (MSSS) soumettait à la Commission pour avis le *Cadre global de gestion sur la sécurité des actifs informationnels du réseau de la santé et des services sociaux.* Ce cadre global vise à uniformiser les pratiques en matière de sécurité dans le réseau de la santé et des services sociaux et à garantir la prise en charge, par l'ensemble des organisations du réseau, de la protection des informations numériques. Un cadre de sécurité est un élément structurant dans l'atteinte d'une protection des renseignements personnels adéquate et nous soulignons notre intérêt pour cette initiative.

Le cadre global de sécurité s'inscrit dans un projet d'élaboration d'un cadre de gestion plus large qui portera sur la protection des renseignements personnels et la gestion du consentement. Cette démarche rejoint nos préoccupations d'encadrer la protection des renseignements personnels sous un angle plus globalisant et complet afin que soient pris en charge tous les aspects des règles fondamentales de protection des renseignements personnels. Nous insistons sur l'importance pour le Ministère d'avoir choisi d'aborder la protection des renseignements personnels comme un enjeu plus large que la stricte sécurité. Bien que les règles fondamentales de protection des renseignements personnels en matière de cueillette, de conservation, d'utilisation, de communication et de destruction puissent être supportées par des mesures de sécurité, la sécurisation n'est pas un préambule à la légitimité d'une cueillette, d'une utilisation ou d'une communication de renseignements personnels. Par ailleurs, la sécurisation ne doit pas induire des possibilités d'atteinte à la vie privée des utilisateurs d'une technologie.

Le cadre global comprend une politique nationale sur la sécurité, la détermination des rôles et responsabilités des intervenants, une série de mesures de sécurité obligatoires et un guide opérationnel contenant des mesures de sécurité facultatives. Le présent avis apporte des commentaires et suggestions sur le contenu du cadre global de sécurité. Une vision globale d'appréciation du cadre global de sécurité sera brossée en conclusion.

1. LA PORTÉE DU CADRE GLOBAL

Le cadre global présenté concerne la sécurité des informations électroniques. Bien que l'information sous forme numérique soit de plus en plus répandue, le papier conserve toujours une place importante dans bon nombre d'institutions québécoises; pensons seulement aux dossiers papiers, aux extrants de systèmes et au principe d'interchangeabilité des supports. Des dispositions particulières peuvent, certes, s'appliquer aux informations numériques, mais nous croyons qu'un cadre de sécurité qui se veut global devrait permettre d'assurer la protection des données indépendamment du support.

D'autre part, les organismes assujettis au cadre de sécurité sont le MSSS, les régies régionales et les établissements. Le réseau de la santé et des services sociaux (RSSS) regroupe un grand nombre de partenaires qui ne seront pas soumis à ce cadre de sécurité. Qu'advient-il alors des renseignements personnels qui se trouvent dans une clinique privée, une pharmacie ou un organisme communautaire? Et qu'en est-il de la SOGIQUE qui assure

l'interopérabilité des technologies, établit les normes techniques et réalise le développement des systèmes dans le RSSS?

2. L'APPLICATION DU CADRE GLOBAL

Afin de s'assurer que le cadre global de sécurité soit respecté par tous les organismes assujettis, il importe que son application soit légalement imposée. Le MSSS, en regard des actifs informationnels, a des pouvoirs de réglementation particuliers précisés dans la *Loi sur les services de santé et les services sociaux* :

> ***520.4.*** *Le ministre peut prendre un règlement sur les normes de sécurité requises pour assurer la confidentialité et la sécurité de l'information électronique, applicable aux régies régionales, aux établissements et à toute personne qui utilise les actifs informationnels du réseau de la santé et des services sociaux.*
>
> *Le règlement spécifie les dispositions de celui-ci dont la contravention constitue une infraction.*

Ce pouvoir réglementaire pourrait être utilisé afin que soient légalement imposées les normes de sécurité propres à assurer l'uniformité des pratiques en matière de sécurité.

3. LES RÔLES ET RESPONSABILITÉS DES ACTEURS

3.1 LA RESPONSABILITÉ DES ACTIFS ET LA COORDINATION DE LA SÉCURITÉ

Le cadre global détermine les rôles et responsabilités des divers intervenants du réseau de la santé dans la mise en œuvre d'une structure organisationnelle de la sécurité. Cette structure est pyramidale et comporte trois niveaux : national, régional et local.

La responsabilité et l'imputabilité en matière de protection des renseignements personnels et de sécurité font référence à la notion de détention juridique des fichiers de renseignements personnels. La responsabilité de l'actif informationnel en matière de sécurité est donc nécessairement locale. Afin d'éviter toute confusion, nous souhaiterions voir distinguer l'attribution des responsabilités en regard des actifs, des rôles de coordination qui peuvent s'exercer sans référence aux actifs eux-mêmes. Ainsi, les responsables régionaux et le responsable national jouent un rôle de coordonnateurs et devraient être désignés coordonnateurs.

D'autre part, le cadre global réfère aux « actifs informationnels du RSSS ». Or, les règles de protection des renseignements personnels au Québec s'exercent en fonction du cloisonnement des organismes publics. *La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, ci-après Loi sur l'accès,

commande à chaque organisme public d'assurer la protection des renseignements personnels dont il est le détenteur légal. Afin d'éviter toute confusion à cet égard, nous souhaitons que le cadre global traite d'actifs informationnels des organismes publics plutôt que d'actifs informationnels du réseau.

3.2 LE COMITÉ NATIONAL PERMANENT DE SÉCURITÉ ET LES AUTRES COMITÉS

Le cadre global prévoit la constitution d'un comité national permanent de sécurité (CNPS). Il est toutefois muet quant à la composition du CNPS. Celle-ci nous apparaît stratégique et devrait réunir des représentants de divers secteurs d'activités (direction, informatique, vérification interne et audit, utilisateurs, service juridique, service de protection des renseignements personnels) et des divers niveaux de responsabilité (national, régional et local).

En 1998, lorsque la Commission a dressé un portrait de la sécurité des ministères et organismes gouvernementaux par l'application de la méthode Marion, la démarche prescrivait la mise sur pied d'un comité local de sécurité. Au terme de cet exercice, la Commission recommandait aux organismes de maintenir en place le comité de sécurité afin d'assurer la pérennité de la démarche de sécurité amorcée par son intervention. Ce type de comité est d'un apport considérable dans une démarche de sécurité, puisque ses intérêts sont directement liés aux actifs à protéger. Aussi, nous suggérons que soit évaluée l'opportunité d'intégrer à la structure, décrite au plan global, des comités locaux de sécurité.

3.3 LA RÉGIE DE L'ASSURANCE MALADIE DU QUÉBEC

Lorsque la Régie de l'assurance maladie du Québec (RAMQ) fournit des services d'entreposage de données au MSSS en vertu de l'article 2 de la *Loi sur la Régie de l'assurance maladie du Québec*, elle se doit de mettre en place les règles de sécurité applicables aux données qu'elle entrepose pour le compte du Ministère. Dans ce cas, nous croyons que le cadre global de sécurité doit être appliqué par la RAMQ afin de maintenir, le cas échéant, le niveau de sécurité dont jouiraient ces banques si elles demeuraient au MSSS.

3.4 LE RESPONSABLE LOCAL DE LA SÉCURITÉ

Le cadre global assigne au responsable local de la sécurité, notamment la responsabilité d'élaborer une politique locale de sécurité et de coordonner sa mise en œuvre.

Le cadre global précise des principes importants en sécurité dont quelques-uns ne sont toutefois pas exprimés en terme de responsabilités. Ceux-ci devraient être assignés au responsable local de sécurité; à titre d'exemple, la mise à jour de la politique, la mise en œuvre d'un programme de sensibilisation et de formation.

3.5 LE RESPONSABLE DE L'ACCÈS

Nous constatons que le rôle du responsable de l'accès a été formalisé dans la structure de sécurité établie par le cadre global de sécurité. Son rôle est de collaborer avec le responsable de sécurité afin de s'assurer du respect des principes de protection des renseignements personnels. Ce rôle pourrait être élargi afin qu'il s'assure que l'introduction d'une nouvelle technologie n'induit pas de risque quant à la vie privée des utilisateurs de celle-ci.

3.6 LE DÉTENTEUR DES ACTIFS

Le détenteur d'un actif en assure la sécurité. Afin d'assumer ce rôle, nous croyons que ce dernier devrait être impliqué dans toute la démarche de sécurité, notamment en ce qui a trait à l'évaluation des risques, à la détermination du niveau de protection actuel et visé, à la détermination des contrôles non informatiques (en amont et en aval) et à la prise en charge des risques résiduels.

Le cadre global précise que le détenteur *propose* les règles d'accès aux actifs. Puisqu'il en assume la responsabilité en matière de sécurité, nous croyons qu'il devrait plutôt déterminer les règles d'accès et autoriser les accès aux seuls utilisateurs qui en ont besoin dans l'exercice de leur fonction et uniquement après avoir l'assurance que les exigences de sécurité seront respectées. La procédure de gestion des droits d'accès devrait être consignée et la responsabilité de l'octroi d'un accès devrait relever du détenteur de l'actif.

3.7 LES UTILISATEURS

Le cadre global énonce que les utilisateurs doivent appliquer et respecter toutes politiques, mesures et procédures en matière de sécurité des actifs informationnels et appliquer les lois et règlements spécifiques à leur domaine. Les utilisateurs doivent aviser leur supérieur immédiat de toute situation portée à leur connaissance et qui est susceptible de compromettre la sécurité des actifs informationnels de l'organisme.

Afin que les utilisateurs puissent remplir leurs obligations, elles devront leur être signifiées d'une façon claire. Dans le cadre du programme de sensibilisation qui pourra être confié au responsable local de la sécurité, ils pourront être informés du contenu de leurs obligations en matière de sécurité et de protection des renseignements personnels.

4. LA REDDITION DES COMPTES

Le cadre global institue une procédure de reddition des comptes en matière de sécurité vers le haut de la structure pyramidale. L'établissement doit soumettre des bilans et des rapports de l'état de la sécurité de l'établissement au coordonnateur régional. Ce dernier doit produire tous les rapports requis à l'intention du coordonnateur national afin que celui-ci puisse réaliser les bilans nationaux de l'état de situation en matière de sécurité.

L'objectif visé par cette procédure de reddition des comptes ne nous apparaît pas clairement défini. Veut-on s'assurer de la mise en œuvre du cadre global de sécurité ou veut-on apprécier le niveau de sécurité de chaque établissement?

Dans cette dernière perspective, nous nous interrogeons sur la conciliation possible entre l'atteinte d'un niveau de sécurité global et le respect de l'autonomie des établissements qui sont responsables et imputables de la sécurité de leurs actifs et du choix des moyens à mettre en œuvre localement.

D'autre part, nous sommes préoccupés par la nature des renseignements qui circuleront dans la structure afin de produire les bilans et rapports de sécurité. L'information relative à la sécurité des actifs est usuellement traitée de façon confidentielle. Nous nous inquiétons des effets d'une éventuelle concentration des vulnérabilités des systèmes d'information du réseau de la santé par région et centralement. La circulation de ce type d'information et sa concentration induit des risques supplémentaires quant à la protection des renseignements personnels.

5. LA DÉMARCHE DE SÉCURITÉ

Le cadre global établit une série de principes directeurs qui visent à procurer aux acteurs impliqués une compréhension commune de la sécurité et des moyens à mettre en œuvre afin d'atteindre un niveau de sécurité adéquat.

Les principes directeurs énoncés proposent une démarche opérationnelle de sécurité qui ne couvre pas, à notre avis, l'ensemble des activités généralement reconnues en matière de sécurité. À cet effet, les activités de mise en œuvre de la structure organisationnelle, de planification, de réalisation, de suivi, de contrôle et de vérifications ou audits méritent d'être distinguées et précisées. De plus, les évaluations des risques, pour être crédibles, doivent se faire avec une méthode conçue à cette fin et reconnue par le milieu. Les réévaluations, quant à elles, doivent être récurrentes et leur fréquence doit être imposée.

6. LA CLASSIFICATION DES DONNÉES ET DES ACTIFS INFORMATIONNELS

La démarche de sécurité proposée dans le cadre global précise qu'afin de déterminer les mesures de sécurité à mettre en place, les actifs informationnels doivent faire l'objet d'une classification selon leur valeur et leur sensibilité. On y décrit à titre de pratique recommandée un mode de classification des actifs informationnels.

> « ...
> - *les données sont classifiées selon le niveau approprié de confidentialité, d'intégrité et de disponibilité;*

- *les actifs informationnels sont classifiés en fonction de la nature des données que l'actif traite ou emmagasine;*
- *la classification des données s'effectue telle qu'énoncée ci-dessous :*
  - *caractère critique pour l'organisme : activité qui caractérise le mieux l'actif :*
    - *incidence sur la qualité des services donnés aux usagers;*
    - *contraintes ou obligations légales;*
    - *impact sur les engagements formels;*
    - *véhicule des informations décisionnelles sur l'organisation;*
    - *gestion des ressources humaines;*
    - *gestion des ressources financières;*
    - *soutien des travaux de l'administration;*
    - *autres;*
  - *caractère confidentiel de l'information : niveau de confidentialité de l'information :*
    - *nominative (concerne une personne physique et permet de l'identifier);*
    - *confidentielle ou stratégique (sous le sceau du secret);*
    - *publique (accessible à tous).*

Note :

- *Les données personnelles peuvent se retrouver dans l'une ou l'autre des trois catégories.*
- *De même, les données de nature sensible peuvent se retrouver dans l'une ou l'autre des trois catégories.* »

La classification des actifs informationnels en fonction de la nature de l'information est une pratique nouvelle pour la Commission. La Loi sur l'accès n'attribue pas de niveau de sensibilité aux renseignements personnels. La catégorisation des renseignements en fonction de leur nature pourrait induire une banalisation non souhaitée de certains types de renseignements et ceux-ci pourraient ainsi se voir offrir une protection inadéquate. La protection des renseignements personnels n'est pas directement fonction de la nature de l'information elle-même, mais répond à un ensemble beaucoup plus complexe de règles.

> « *Il est insuffisant de mettre en place des mesures de sécurité si l'on ne prend pas la peine d'identifier les risques de se retrouver en contravention des lois.* »[1]

Par ailleurs, l'exercice de classification décrit au cadre global recommande un réaménagement et un regroupement des données en fonction de la classification de l'information.

[1] Pierre Trudel, CRDP, allocution « Aspects juridiques des technologies de l'information », avril 2001.

La cueillette de renseignements personnels par un organisme est subordonnée à l'existence d'une finalité connue et ces renseignements ne peuvent être utilisés que pour cette seule finalité. Le cloisonnement des fichiers de renseignements personnels à l'intérieur d'un organisme en fonction des finalités fait partie des garanties de confidentialité et de respect de la vie privée prévues par le législateur. Le réaménagement et le regroupement de données ne doivent pas réduire l'application du principe fondamental du respect des finalités de la cueillette.

7. LES MESURES DE SÉCURITÉ

La section III du cadre global établit une liste de mesures de sécurité imposées aux organismes assujettis au cadre global de sécurité.

Un cadre de sécurité vise à mettre en place une structure afin que la sécurité soit prise en charge localement. Un cadre global établit des objectifs de sécurité, les moyens étant par ailleurs laissés à la discrétion des premiers responsables, les détenteurs.

Il nous apparaît risqué de réduire une démarche de sécurité en une liste de mesures de sécurité à appliquer. Une telle liste peut devenir impossible d'application pour un petit organisme et nettement insuffisante pour un gros organisme. Signalons par ailleurs que la section III est muette sur certains aspects stratégiques en matière de sécurité (par exemple, l'appréciation des contrôles permanents, de l'aspect économique et humain, de la sensibilisation particulière du personnel informatique, de l'attribution des tâches incompatibles, des procédures de recettes en exploitation, des méthodes d'analyse, de programmation et les jeux d'essais…). De plus, des sujets soulevant des enjeux en matière de protection des renseignements personnels sont absents, tels que le contrôle des extrants, la sécurité des portables, la sécurité des transmissions, le respect du cloisonnement des organismes, le télé-entretien, le télétravail et l'utilisation des réseaux ouverts.

Bien que des normes minimales puissent être établies dans un contexte particulier (par exemple, des conditions peuvent être établies pour un branchement au RTSS ou pour utiliser une application particulière), nous croyons que l'énumération d'une série de mesures de sécurité sorties de leur contexte banalise et minimise le besoin de recourir à une évaluation rigoureuse des menaces et des risques.

Le niveau de détail des mesures énumérées dans le cadre global est variable. Nous percevons certaines mesures de sécurité comme des *objectifs* de sécurité alors que d'autres sont décrites avec un niveau de détail qui approche le *moyen*. Les objectifs de sécurité sont universels mais les moyens varient en fonction de divers critères notamment le domaine d'activité, la taille de l'organisation et l'architecture des systèmes.

Nous suggérons que les objectifs de sécurité se reflètent en terme de rôle et de responsabilité des différents acteurs. Par exemple, afin que la sécurité soit prise en charge dans le processus d'acquisition de logiciels, un principe doit être établi à cet effet et le respect de

celui-ci doit être assuré par un acteur. De même, la tenue des registres d'autorité, d'incidents et d'actes de gestion de la sécurité doit être sous la responsabilité d'une personne.

Afin d'assurer que la sécurité soit réellement opérationnelle, nous croyons que le MSSS aurait avantage à fournir une véritable méthode d'analyse de risques reconnue. De nombreuses méthodes existent. Une méthode d'analyse des risques efficace et fiable évolue en fonction des nouveaux risques et des NTIC. Rappelons en regard des risques résiduels que le gouvernement a, à l'égard de la protection des renseignements personnels, une obligation de résultats. C'est pourquoi, l'État ne peut consciemment mettre en péril des données personnelles pour des questions économiques ou autres.

À cet égard, l'expérience Marion nous a permis de constater que les organismes, particulièrement les petits, sont plutôt démunis en terme de méthodes et disposent de peu de ressources afin de supporter leur démarche d'évaluation des risques.

8. CONCLUSION

Le déploiement d'un cadre global de sécurité et l'élargissement éventuel de ce cadre afin de tenir compte de la protection des renseignements personnels représentent une initiative structurante dans l'atteinte d'un niveau adéquat de protection des renseignements personnels.

Les présents commentaires visent à bonifier le cadre global soumis, lequel sera, nous l'espérons, un premier pas vers une démarche que nous souhaitons plus englobante et étendue afin que les renseignements de santé, au Québec, reçoivent une protection uniforme et adéquate.

Aussi, une portée plus large du cadre global quant aux organismes du réseau de la santé assujettis et quant aux types de supports de l'information permettrait d'obtenir une assurance plus grande quant à l'uniformité de la protection des renseignements personnels. L'exercice par le ministre du pouvoir réglementaire offrirait une garantie d'application essentielle d'une démarche de sécurité commune.

L'utilisation d'une méthode d'analyse des risques reconnue et la bonification de la démarche de sécurité proposée procureraient une assurance raisonnable de la prise en charge effective de la sécurité locale.

Le processus de reddition des comptes devra quant à lui être défini dans la perspective du respect du caractère confidentiel et stratégique de l'information sur la sécurité.

Finalement, le rétablissement des liens entre les actifs informationnels et les organismes détenteurs permettra de voir consacrer le principe fondamental du respect du cloisonnement des organismes publics.