Volet Infrastructures

Guide de l'infonuagique

Volume 2 – Considérations en protection des renseignements personnels

Architecture d'entreprise gouvernementale 3.0

Québec

Volet Infrastructures

Guide de l'infonuagique

Volume 2 – Considérations en protection des renseignements personnels

Architecture d'entreprise gouvernementale 3.0

« Pour une utilisation responsable de l'infonuagique au gouvernement du Québec »

Cette publication a été réalisée par
le Sous-secrétariat du dirigeant principal de l'information
et produite en collaboration avec la Direction des communications
du Secrétariat du Conseil du trésor.

Vous pouvez obtenir de l'information au sujet
du Conseil du trésor et de son Secrétariat
en vous adressant à la Direction des communications
ou en consultant son site Web.

Direction des communications
Secrétariat du Conseil du trésor
5e étage, secteur 500
875, Grande Allée Est
Québec (Québec) G1R 5R8

Téléphone : 418 643-1529
Sans frais : 1 866 552-5158

communication@sct.gouv.qc.ca
www.tresor.gouv.qc.ca

Dépôt légal – novembre 2014
Bibliothèque et Archives nationales du Québec

ISBN 978-2-550-71196-4 (en ligne)

Tous droits réservés pour tous les pays.
© Gouvernement du Québec –2014

Table des matières

Liste de sigles et acronymes

AIPRP	Accès à l'information et protection des renseignements personnels
BS	Besoin spécifique
CARRA	Commission administrative des régimes de retraites et d'assurances
CSPQ	Centre de services partagés du Québec
DIC	Disponibilité, intégrité, confidentialité
DPI	Dirigeant principal de l'information
FISA	*Foreign Intelligence Surveillance Amendments*
IAAS	*Infrastructure as a Service*
MAMROT	Ministère des Affaires municipales, des Régions et de l'Occupation du territoire
MAPAQ	Ministère de l'Agriculture, des Pêcheries et de l'Alimentation du Québec
MCE	Ministère du Conseil exécutif
MELS	Ministère de l'Éducation, des Loisirs et des Sports
MESS	Ministère de l'Emploi et de la Solidarité sociale
MJQ	Ministère de la Justice du Québec
MTQ	Ministère des Transports du Québec
PAAS	*Platform as a Service*
PRP	Protection des renseignements personnels
RAMQ	Régie de l'assurance maladie du Québec
SAAS	*Software as a Service*
SCT	Secrétariat du Conseil du trésor
SSDPI	Sous-secrétariat du dirigeant principal de l'information
OP	Organisme public
RI	Ressources informationnelles
TI	Technologies de l'information

Avis

Le présent document intitulé Guide de l'infonuagique – Volume 2 ne constitue pas un manuel de gestion de projet ni un avis juridique, et il ne peut prétendre se substituer aux textes des lois en vigueur. Nous invitons les organismes publics à adresser leurs commentaires et leurs suggestions afin d'améliorer ce guide au Sous-secrétariat du dirigeant principal de l'information, responsable de son élaboration.

Le terme « organisme public » (OP) est utilisé selon la désignation qui en est faite dans la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. Cependant, l'utilisation de ce guide peut être élargie à d'autres organisations telles que les entreprises du gouvernement et les municipalités.

À noter que le terme « fournisseur » utilisé dans ce document réfère à la notion de prestataire de services.

Ce document sera révisé périodiquement.

Avant-propos

Au cours des dernières décennies, l'apport des technologies de l'information (TI) pour les organismes publics (OP) a été indéniable. Levier de transformation organisationnelle par excellence, ces technologies ont permis des améliorations notables au regard de la prestation de services aux citoyens.

Notion relativement récente, l'infonuagique (*cloud computing*) présenterait aussi des possibilités avantageuses pour les OP dans la gestion de leurs ressources informationnelles (RI) : possibilités de mise en commun, de partage, de réutilisation, entraînant agilité, économies d'échelle, etc.

Aux avantages qu'offre cette nouvelle façon d'acquérir des ressources en TI, s'opposent, comme c'est le cas lors de l'avènement de nouvelles technologies, certaines préoccupations. En effet, cette notion est encore méconnue et parfois même, sujette à appréhension, en raison notamment de la perception des risques qu'elle suscite. La protection des renseignements personnels et la sécurité des données figurent parmi les préoccupations liées à cette solution. Bien que réels, ces risques peuvent néanmoins être circonscrits et maîtrisés de différentes façons et permettre ainsi que la confiance du public envers les organismes qui y ont recours soit maintenue.

Les Guides de l'infonuagique (Volume 1 à 4) constitue un outil de référence pour l'OP qui envisage d'avoir recours à l'infonuagique. Il met en lumière les différentes caractéristiques de ce nouveau mode de prestation de services, et propose une démarche et des étapes à suivre pour y recourir. Dans l'élaboration de ses besoins, l'organisme devra déterminer quel service infonuagique et quel mode de déploiement conviennent le mieux en fonction, notamment, de la nature (portée, effets sur l'organisation, etc.) du service qu'il souhaite acquérir et du type d'information à héberger dans le nuage. Selon les réponses obtenues, il pourra, si nécessaire, aborder de multiples approches pour faire face aux risques que peut présenter cette technologie, comme appliquer différents niveaux de sécurité en fonction de la sensibilité des données hébergées, ou préférer l'utilisation d'un « nuage privé », géré à l'interne ou par un fournisseur, pour n'en nommer que quelques-unes.

Les utilisateurs de ce guide doivent garder à l'esprit qu'il n'existe pas de recette unique pour acquérir un service infonuagique. Les modèles de services (infrastructure, plateformes de développement, logiciels, etc.), les modes de déploiement (privé, public, communautaire, hybride) et l'ampleur des projets peuvent être si variables que les mesures de mitigation des risques sont uniques à chaque projet, en fonction du contexte de chaque organisation. Le présent fascicule intitulé Volume 2 –Considérations sur la protection des renseignements personnels permet néanmoins d'informer les parties prenantes sur les enjeux communs, notamment en ce qui a trait à la protection des renseignements personnels ou confidentiels, à

la sécurité de l'information et au processus de négociation et de gestion des contrats de services infonuagiques.

Afin d'assurer une utilisation responsable de l'infonuagique, l'adoption graduelle devrait être préconisée pour la mise en place de ce nouveau mode de prestation en TI. Ceci permettra aux organismes, projet après projet, d'en évaluer les bénéfices, de s'approprier les nouveaux paramètres applicables aux différentes solutions en constante évolution et, finalement, de développer l'expertise nécessaire à la réussite de leurs projets futurs.

Le présent volume du guide de référence de l'infonuagique a été réalisé avec la collaboration de nombreux rédacteurs représentant plusieurs OP dont voici la liste :

Cynthia Morin	CSPQ	Gaston Brumatti	MELS
Dave Tanguy	SCT	Mathieu Dufour	RAMQ
Denyse Roussel	MCE		

Ce document a fait l'objet d'un cycle de validation par les intervenants suivants :

Christian Boisvert	MJQ	Marc Bellavance	MAPAQ
Daniel Bouchard	MTQ	Patrick Boisvert	CARRA
Éric Gagnon	MAPAQ	Pierrette Brie	MESS
Fernande Rousseau	MCE	Stéphane Asselin	CSPQ
Ghislain Dubé	MJQ	Yvan Boulet	MAPAQ
Hugues Beaudoin	RAMQ	Yvon Gagné	MAPAQ
Jean-François Ducré-Robitaille	MAMOT		

Parallèlement aux travaux d'élaboration de ce guide, le gouvernement du Québec a mandaté le Centre de recherche en droit public de l'Université de Montréal pour la réalisation d'une étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement québécois. Cette étude se veut une analyse des risques et des contraintes juridiques associés à l'infonuagique. Outre les éléments juridiques soulevés dans cette étude, notamment ceux relatifs à la sécurité de l'information dans le contexte d'un service infonuagique, il est important de considérer l'ensemble des principes et des obligations de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (ci-après : la « Loi sur l'accès »). À cet égard, il y aura lieu de se référer au responsable de l'accès à l'information et protection des renseignements personnels (AIPRP) de chaque organisme.

1. Introduction

L'infonuagique (*cloud computing*) constitue une tendance mondiale en matière d'acquisition de services technologiques dont l'un des objectifs est de diminuer les coûts d'exploitation des infrastructures technologiques et des applications. Il s'agit d'un nouveau mode d'acquisition qui permet aux individus et aux organisations d'accéder, par les technologies d'Internet, à un bassin de ressources informatiques configurables, externalisées et qui sont proposées sous forme de services. Ce nouveau mode de livraison de services permet aux consommateurs de s'approvisionner en services de technologies de l'information (TI) auprès d'un fournisseur infonuagique de façon automatisée et sur demande. La consommation des services est mesurée et facturée selon l'utilisation. L'infonuagique procure plusieurs avantages et bénéfices aux utilisateurs. En effet, les ressources infonuagiques offrent une agilité et une flexibilité à l'utilisation puisqu'elles s'acquièrent rapidement, s'adaptent facilement à la demande et permettent un délestage tout aussi rapide. De plus, l'infonuagique présente des possibilités de faire des économies substantielles, puisqu'elle favorise une meilleure utilisation des infrastructures technologiques, réduisant les coûts en capitalisation, en exploitation et en entretien à l'échelle gouvernementale.

Plusieurs gouvernements, dont ceux des États-Unis, du Royaume-Uni et de l'Australie, considèrent que l'infonuagique est un levier de transformation et d'économie important. D'ailleurs, ces pays ont mis sur pied des stratégies d'adoption et leurs initiatives infonuagiques gouvernementales sont nombreuses. Malgré les possibilités intéressantes qu'offre l'infonuagique, il existe des préoccupations et des risques inhérents à son utilisation, tant sur le plan juridique, notamment en ce qui concerne la propriété matérielle et intellectuelle et les obligations de protection des renseignements personnels (PRP), qu'en ce qui a trait à la sécurité des données.

Afin de bien tirer profit des bénéfices et de saisir pleinement les possibilités rattachées à l'infonuagique, le dirigeant principal de l'information (DPI) a mandaté un groupe de travail interministériel dont l'objectif consistait à réaliser ce guide de référence fournissant l'information nécessaire pour une utilisation responsable de l'infonuagique et un ensemble de bonnes pratiques en la matière.

1.1 Objectifs et portée du guide

Compte tenu de l'intérêt croissant pour l'infonuagique au sein des organisations, l'objectif de ce guide est de fournir des informations pertinentes aux OP qui désirent recourir à de tels services afin d'encadrer cette pratique de façon appropriée et sécuritaire. Ce guide vise, entre autres, les objectifs suivants :

- ✓ Offrir de l'information sur la signification et la portée des services infonuagiques;
- ✓ Proposer des questions à se poser et des pratiques à considérer, telles que :
  - La prise en compte des enjeux et des risques qui sont associés au projet dès les premières étapes d'analyse préliminaire ou d'étude d'opportunité et tout au long de sa réalisation;
  - Le respect des exigences en matière de protection des renseignements personnels ou autrement confidentiels, et de sécurité de l'information;
  - La réglementation contractuelle applicable et la gestion des services infonuagiques;
  - La gestion de projet.

Ce guide peut être utilisé par les différents intervenants d'un projet lorsque l'OP envisage de recourir à des services infonuagiques. Il est destiné à les accompagner dans leur démarche d'analyse, d'évaluation et d'encadrement légal et administratif. Son utilisation facilitera la prise de décision quant à l'opportunité de

recourir à des services infonuagiques et aux mesures à mettre en place pour en assurer une utilisation responsable et sécuritaire.

Exemples de questions auxquelles le guide se propose d'apporter des éléments de réponse

- ✓ Quels sont les avantages de l'infonuagique par rapport aux solutions traditionnelles?
- ✓ Quels sont les services, les traitements et les données susceptibles de migrer vers l'infonuagique?
- ✓ Quels sont les risques à maîtriser?
- ✓ Quelles sont les considérations juridiques et les exigences de PRP à respecter?
- ✓ Quelles sont les exigences de sécurité de l'information à prendre en compte?
- ✓ Comment définir les termes contractuels et sélectionner un fournisseur infonuagique?

Enfin, ce guide met l'accent sur les éléments particuliers à considérer dans le cas de recours à des services infonuagiques. Il ne traite pas de façon exhaustive de toutes les considérations juridiques ou administratives ni des normes et des bonnes pratiques qui s'appliquent à tout projet en ressources informationnelles réalisé par un OP. Il y aura donc lieu de s'assurer que ces divers éléments sont pris aussi en considération dans le projet ciblé.

1.2 Présentation du contenu

Ce document intitulé Volume 2 – Considérations en protection des renseignements personnels est le deuxième de quatre volumes. Il présente les considérations juridiques et les éléments essentiels relatifs aux obligations de protection des renseignements personnels ou autrement confidentiels.

Quant aux autres volumes (1, 3 et 4) du guide de référence, ils sont constitués de sections détaillées qui approfondissent divers enjeux relatifs à l'infonuagique, notamment les notions fondamentales de l'infonuagique (volume 1), celles liées au contrôle et à la sécurité (volume 3) et à la gestion contractuelle (volume 4). Ils ont été développés dans le but d'outiller et d'orienter les spécialistes en informatique ainsi que ceux de la sécurité et de la gestion contractuelle des OP dans l'analyse et l'évaluation des risques.

2. Considérations juridiques et protection des renseignements personnels ou autrement confidentiels

La notion d'infonuagique n'a pas encore été définie par le législateur québécois ou même par les tribunaux. Elle bénéficie toutefois déjà d'un certain encadrement qu'il est préférable de connaître lorsque l'on songe à mettre en place un tel mode d'impartition. Même s'il est possible que d'autres règles s'y appliquent, cette section en présente les éléments incontournables. Une bonne pratique serait également de consulter les services juridiques de votre organisation pour toute question de cette nature afin de vous assurer que tout a été mis en œuvre au regard de ces considérations car tout comme les technologies de l'information, le droit est un domaine en constante évolution.

Les principales considérations juridiques à prendre en compte sont les suivantes : la gouvernance et la gestion des ressources informationnelles, la propriété matérielle et intellectuelle, l'accès et la protection des renseignements personnels ou autrement confidentiels, la sécurité de l'information et la gestion documentaire et contractuelle.

De plus, il faut bien évidemment garder à l'esprit, qu'à l'exception des obligations touchant la gouvernance et la gestion des ressources informationnelles, les règles présentées ici, devraient être adaptées en fonction du modèle pour lequel aura opté l'OP et aussi du type de données qui y seront hébergées. À ce titre, il serait important de se référer à l'Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec[1] qui présente les avantages et les inconvénients de chacun des principaux modèles de déploiement.

2.1 La gouvernance et la gestion des ressources informationnelles

La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement[2] établit un cadre de gouvernance et de gestion en matière de ressources informationnelles, applicable aux ministères et à la plupart des OP, y compris à ceux du réseau de l'éducation et à ceux du réseau de la santé et des services sociaux. En vertu de cette loi, une ressource informationnelle est utilisée par un OP, dans le cadre de ses activités de traitement de l'information, pour mener à bien sa mission et faciliter la prise de décision ou la résolution de problèmes.

Cette loi oblige les organismes assujettis à faire autoriser leurs projets en matière de ressources informationnelles par, selon le cas, le gouvernement, le Conseil du trésor, le ministre de l'Éducation, du Loisir et du Sport, le ministre de la Santé et des Services sociaux, ou le conseil d'administration de l'OP ou, à défaut d'un tel conseil, par le plus haut dirigeant de l'organisme. Les entreprises du gouvernement, quant à elles, doivent adopter une politique basée sur les objectifs énoncés dans cette loi. De plus, les règles relatives aux demandes d'autorisation de projets et aux outils de gestion en ressources informationnelles[3] précisent les conditions et les modalités de suivi et de reddition des projets et activités en ressources informationnelles des OP, comme la production annuelle de la planification triennale des projets et des activités en ressources informationnelles, la programmation annuelle des ressources informationnelles et le bilan annuel des réalisations en ressources informationnelles. Ainsi, il est important

1. Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI. Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec, Centre de recherche en droit public, 2014.
2. Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, RLRQ, chapitre G-1.03.
3. Recueil des politiques de gestion, vol. 11, 2, 2, 6 (Publication Québec).

que tout projet en infonuagique fasse l'objet d'une évaluation du processus d'autorisation auquel il est soumis.

2.2 La propriété matérielle et intellectuelle

Au chapitre de la propriété matérielle, l'OP devrait veiller à prévoir dans ses clauses contractuelles ce qu'il entend conserver et ce que le prestataire de services devrait lui transférer. Quant à la propriété intellectuelle, l'OP devra garder un œil bienveillant à cet égard, puisque l'utilisation de l'infonuagique touche à quelques-uns de ses aspects.

Se définissant comme l'ensemble des droits qui découlent de l'activité intellectuelle dans les domaines industriel, scientifique, littéraire et artistique, la propriété intellectuelle peut prendre la forme d'un brevet, d'une marque de commerce, d'un droit d'auteur, d'un dessin industriel, ou encore, d'une topographie de circuits intégrés, pour lesquels il existe une loi fédérale propre à chacun. Les Normes en matière d'acquisition, d'utilisation et de gestion de droits d'auteurs des documents détenus par le gouvernement, les ministères et les organismes publics désignés par le gouvernement[4] de même que le Cadre de gestion et de valorisation de la propriété intellectuelle[5] guideront également les OP dans la planification de la protection de la propriété intellectuelle.

De façon plus spécifique, l'OP devrait s'assurer que les clauses contractuelles lui permettent et lui garantissent une utilisation adéquate du service infonuagique adaptée à ses besoins. Il est à noter que dans les cas de contrats d'adhésion pour certains services d'infonuagique de type public, par exemple, cette assurance peut être plus difficile à obtenir. Également, le prestataire devrait garantir à l'OP qu'il détient les droits de propriété intellectuelle nécessaires et qu'il a reçu les autorisations requises pour la réalisation du contrat, tout comme l'OP, qui doit lui garantir qu'il détient les droits nécessaires pour accorder une licence. Les clauses contractuelles devraient également prévoir une cession ou une licence de droits d'auteur sur les travaux du prestataire et, le cas échéant, sur le matériel antérieur ou préexistant.

L'OP devrait également évaluer les risques de clauses, parfois abusives, entre autres dans le cas de l'utilisation de services infonuagiques publics. En effet, certaines clauses élaborées par des prestataires de services infonuagiques précisent que le client, en l'occurrence ici l'OP, conserve ses droits de propriété intellectuelle sur les contenus qu'il soumet au prestataire, mais que ce dernier s'accorde une licence, parfois universelle et même illimitée, d'utilisation, d'hébergement, de stockage, de reproduction, de modification, de création d'œuvres dérivées de communication, de publication, de représentation publique, d'affichage ou de distribution publique de ces contenus. Certaines clauses vont même jusqu'à prévoir une renonciation par l'utilisateur à ses droits moraux.

Par ailleurs, le respect des droits de la propriété intellectuelle constitue un autre enjeu dont l'OP devrait se préoccuper. Puisque la nature du « nuage » peut, dans certains cas, donner lieu à des hébergements dans des localisations diverses et parfois inconnues, il pourrait être difficile de prévoir quelles lois seront applicables, les droits de propriété intellectuelle étant le plus souvent définis en fonction du territoire. De surcroît, en matière de droit d'auteur, ce qui constitue une violation de ce droit dans un pays peut ne pas l'être dans un autre. À noter que le Canada a adhéré à certains traités internationaux, dont la Convention de Berne, qui stipule que les titulaires de droits d'auteur pourraient voir les violations de ces droits survenues dans les pays membres de cette convention, sanctionnées en fonction de leur législation nationale.

Également, les protections accordées aux brevets et marques de commerce ne valent que pour les pays dans lesquels elles ont été accordées. Les détenteurs de brevets ou de marques de commerce doivent en faire protéger la propriété dans tout territoire où ils souhaitent bénéficier de cette protection. Ainsi, des complications pourraient survenir pour les détenteurs de brevets et de marques de commerce, pour l'auteur

4. Gazette officielle du Québec, 25 octobre 2000, 132e année, n°43 (A.M.,2000) p. 6753.

5. Cadre de gestion et de valorisation de la propriété intellectuelle http://www.mesrst.gouv.qc.ca/fileadmin/contenu/publications/RST/dispositions.pdf

et les titulaires de droits d'auteur, ou encore pour les licenciés qui entreprennent de faire respecter leurs droits à l'égard des contrefacteurs.

Par ailleurs, la détermination du titulaire des droits d'auteur, lorsqu'il y a création de nouvelles œuvres dans le cadre des services infonuagiques, représente aussi un enjeu que les OP devraient prendre en compte.

2.3 Vie privée, protection des renseignements personnels et sécurité de l'information

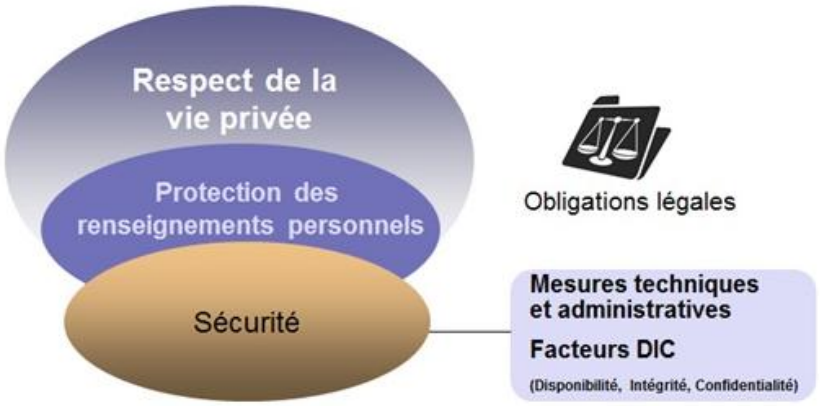
Les notions de respect de la vie privée, de protection des renseignements personnels et de sécurité de l'information[6] sont distinctes, complémentaires et interreliées. Le schéma qui suit montre ces interrelations en faisant ressortir que la sécurité de l'information est une notion distincte de la protection des renseignements personnels et qu'elle est un des moyens d'assurer la protection des renseignements personnels. Elle n'est pas garante de la protection des renseignements personnels au sens de la Loi sur l'accès ou d'une autre loi. Par exemple, dans le cas où des renseignements personnels sont communiqués à un tiers, si une analyse de conformité n'a pas été faite pour déterminer que l'organisation est autorisée à communiquer ces renseignements, cette communication, bien qu'elle puisse se faire de façon sécuritaire, pourrait être illégale. Il est donc important que l'analyse de conformité soit effectuée avant que les mesures de sécurité pour protéger les renseignements personnels ou autrement confidentiels ne soient déterminées[7].

Par ailleurs, la sécurité se réfère à des dimensions qui ne sont pas entièrement régies par la Loi sur l'accès. Ainsi, l'intégration d'un processus de protection des renseignements personnels dans un projet de service infonuagique n'englobe pas toutes les pratiques de sécurité qu'un OP doit mettre en œuvre pour garantir la sécurité de l'information de la solution d'affaires et, inversement, ce processus de protection des renseignements personnels ne couvre pas toutes les exigences de sécurité. Le schéma nº 1 qui suit montre les interrelations entre les notions de vie privée, de protection des renseignements personnels et de sécurité de l'information.

6 Cette section est basée sur le document suivant : Gouvernement du Québec : Denyse ROUSSEL et Denis BISTODEAU, Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics, 2009, version 1,1. [En ligne], http://www.institutions-democratiques.gouv.qc.ca/acces-information/documents/modele-pratique-prp-2009.pdf.

7. Il importe également de considérer l'information autre que personnelle dont la confidentialité doit (restrictions obligatoires) ou peut être protégée (restrictions facultatives) par la Loi sur l'accès et dont la décision relève du responsable de l'accès à l'information et de protection des renseignements personnels. Voir à ce sujet les restrictions à l'accès prévues à la section II de la Loi sur l'accès.

Figure 1: Respect de la vie privée, PRP et sécurité (Modèle de pratique de PRP, Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques)



2.4 L'accès et la protection des renseignements personnels ou autrement confidentiels

Le respect des droits fondamentaux que sont l'accès à l'information et la protection des renseignements personnels (AIPRP), énoncés dans la Loi sur l'accès[8], de même que dans de nombreuses autres lois[9] doit occuper une place de premier plan lors de la planification, de la réalisation et du déploiement d'un service infonuagique pour les OP. Pour ce faire, ces derniers doivent notamment mettre en place les mesures nécessaires pour :

- ✓ Permettre aux personnes d'exercer leur droit d'accès aux documents;
- ✓ Permettre aux personnes d'exercer leur droit d'accès aux renseignements personnels qui les concernent ainsi que leur droit de rectification de ceux-ci;
- ✓ Assurer le respect des principes et des obligations de protection des renseignements personnels et de ceux relatifs à la confidentialité des autres renseignements.

Par ailleurs, l'OP veillera à respecter une obligation issue d'une disposition du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels[10] qui prévoit qu'un OP assujetti doit informer le comité sur l'accès à l'information et sur la protection des renseignements personnels, formé en conformité avec ce règlement, des projets d'acquisition, de développement et de refonte d'un système d'information ou de prestation électronique de services qui recueille, utilise, conserve, communique ou détruit des renseignements personnels. Ce comité suggère, parmi les projets soumis, ceux qui doivent être encadrés par des mesures particulières de protection des renseignements personnels.

8. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, chapitre A-2.1.
9. Loi sur les services de santé et les services sociaux, RLRQ, chapitre S-4.2; Loi sur l'administration fiscale, RLRQ, chapitre A-6.002, pour n'en nommer que quelques- unes.
10. Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ, chapitre A-2.1, r. 2.

2.4.1 La confidentialité des renseignements personnels ou autrement confidentiels

Les OP doivent s'assurer, lorsqu'ils en impartissent le traitement en mode infonuagique, que la confidentialité des renseignements personnels ou autrement confidentiels sera maintenue et respectée. Cela constitue un enjeu majeur pour un OP.

On entend par renseignements confidentiels, notamment, tous les renseignements personnels fournis à l'État par les citoyens; les renseignements détenus par des tiers qui doivent demeurer confidentiels en raison, par exemple, d'un secret industriel, un renseignement industriel, financier, commercial, scientifique, technique ou encore syndical; certains renseignements communiqués à un tiers auquel une obligation de confidentialité est imposée; un renseignement recueilli dans le cadre d'une médiation [11] ou d'une conférence de règlement à l'amiable[12]; tout comme un renseignement communiqué en vertu de certaines lois, telles que la Loi facilitant le paiement des pensions alimentaires[13], la Loi sur la protection de la jeunesse[14], etc.

2.4.2 La protection des renseignements personnels

La protection des renseignements personnels constitue l'une des dimensions du respect de la vie privée. En principe, toute personne a un droit de regard sur les renseignements qui la concernent et qui peuvent être colligés, rendus accessibles, utilisés, communiqués, conservés et détruits par un OP. Ces activités représentent les moments clés du cycle de vie des renseignements personnels.

Il importe de noter que la qualité d'un service infonuagique en matière de protection des renseignements personnels est largement tributaire de la qualité des processus de protection de ces renseignements et de sécurité réalisés en amont et tout au long du projet ainsi que lors de leur intégration dans la gestion du projet.

Les bonnes pratiques de protection de ces renseignements reposent sur un processus basé sur le cycle de vie des renseignements personnels qui reflète toutes les obligations qu'un OP doit respecter. Un processus de protection des renseignements personnels est un ensemble de pratiques regroupées par objectifs qui, lorsqu'elles sont réalisées, permettent d'assurer la protection des renseignements pour l'ensemble de leur cycle de vie. Ce processus, comme tout autre processus à réaliser dans un projet infonuagique, doit être géré dans le projet selon les pratiques éprouvées en gestion de projet. Il peut s'intégrer au processus d'analyse de risque du projet et des risques de sécurité de l'information.

La figure 2 qui suit représente un schéma générique du cycle de vie de la protection des renseignements personnels[15] ainsi que les objectifs spécifiques ou objectifs visés à chacun des moments clés du cycle de vie des renseignements personnels. Un service infonuagique pourrait entraîner de nouveaux flux d'information[16]. Ainsi, le cycle de vie proposé devra être adapté aux flux d'information propres à un service

11. Loi sur les chemins de fer, RLRQ, chapitre. C-14.1.

12. Code de procédure civile, RLRQ, chapitre C-25.

13. Loi facilitant le paiement des pensions alimentaires, RLRQ, chapitre P-2.2.

14. Loi sur la protection de la jeunesse, RLRQ, chapitre P-34.1.

15. Ce schéma est extrait du Modèle de pratique de PRP, Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques, page 24.

16 « Le modèle d'informatique dans les nuages pourrait entraîner la création d'énormes fonds de (nouvelles) données et les mettre à la disposition de l'infomédiaire-fournisseur de services d'informatique dans les nuages. Quand l'infomédiaire a la capacité de voir ce qui se passe à chaque clic, il peut produire un riche flux de données. Même si ce flux de données pourrait être sans rapport avec les opérations dans les nuages originales, il risque d'être utilisé soit par l'organisation soit par l'infomédiaire dans les nuages à des fins qui vont au-delà de celles pour lesquelles le consentement avait été donné au départ » http://www.priv.gc.ca/information/research-recherche/2010/cc_201003_f.asp.

infonuagique au regard des enjeux particuliers qu'il soulève, tout en considérant, le cas échéant, d'autres règles de protection des renseignements personnels qui s'appliquent à l'organisation concernée.

Figure 2: Cycle de vie de la PRP (Modèle de pratique de PRP, Partie 1, Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques)

2.4.3 Démarche encadrant l'application des exigences liées à l'accès à l'information et à la protection des renseignements personnels ou autrement confidentiels

Le processus de protection des renseignements personnels devrait être défini dans un projet de services infonuagiques avec les adaptations requises qui tiennent compte des particularités de l'OP et, le cas échéant, de son régime particulier de protection des renseignements[17]. Sa gestion sera intégrée au processus de gestion de projet décrit dans le plan d'affaires du projet d'infonuagique (voir la section 4.1 du document « Volume 1 – Notions fondamentales »).

La section qui suit propose une démarche pour faciliter l'intégration du respect des exigences de protection des renseignements personnels et d'une disposition du Règlement sur la diffusion de l'information et sur la protection des renseignements personnels[18]. Il y a lieu également de considérer la prise en compte des risques qui y sont associés. Cette démarche prend appui sur le processus de protection des renseignements personnels décrit précédemment et intègre des activités habituellement réalisées par des spécialistes en sécurité, telles la catégorisation de l'information, avec la collaboration des responsables de l'accès à l'information et de la protection des renseignements et la collaboration du détenteur. Il y aura donc lieu d'harmoniser les activités de protection des renseignements personnels décrites avec les activités de

17. Par exemple, la Loi sur les services de santé et les services sociaux, RLRQ, chapitre S-4.2.

18. Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, RLRQ, chapitre A-2.1, r. 2.

sécurité, par exemple avec l'analyse de risques de sécurité[19]. Cette démarche n'est pas exhaustive et elle est appelée à être complétée et bonifiée par les OP, selon les différents modèles de services infonuagiques qu'ils utiliseront.

Les grandes étapes de la démarche proposée pour assurer l'accès et la protection des renseignements personnels ou autrement confidentiels selon la Loi sur l'accès[20]

- ✓ Désignation des parties prenantes relativement à l'encadrement de la PRP et de la sécurité de l'information dans le projet. Description de leurs rôles et responsabilités et de leur formation, le cas échéant.
- ✓ Préparation et planification de la démarche d'évaluation des effets et des risques du projet sur la PRP dès l'étude préliminaire ou l'étude d'opportunité du projet.
- ✓ Catégorisation de l'information, en considérant non seulement la PRP, mais également l'information d'autre nature qui doit aussi demeurer confidentielle[21].
- ✓ Description du cheminement ou du flux de l'information pour l'OP et le fournisseur, y compris sa gestion et sa localisation et les supports ou systèmes visés.
- ✓ Établissement d'un consensus avec la personne responsable de l'AIPRP et un conseiller ou une conseillère juridique quant aux activités réalisées avec les renseignements personnels et l'information autrement confidentielle. Par exemple, s'agit-il d'une transmission, d'un accès, d'une communication, d'un traitement par le fournisseur, si oui à quelle fin? S'agit-il d'une collecte ou d'une saisie par le fournisseur? Qui conservera les données une fois qu'elles seront classées, inactives, etc.?
- ✓ Adaptation du cycle de vie des renseignements personnels en fonction du résultat de l'activité précédente et du flux de l'information propre au projet de services infonuagiques.
- ✓ Analyse du cheminement des informations ou des données pour tout le cycle de vie des renseignements personnels établi, qui est interpellé par le projet, et détermination des exigences légales qui s'appliquent au regard des objectifs et des pratiques proposées dans la figure 2 présenté à la page précédente (volet PRP de la Loi sur l'accès) et des éléments à considérer pour l'exercice du droit d'accès aux documents d'un citoyen (volet accès à l'information de la Loi sur l'accès).
- ✓ Évaluation des effets et des risques du projet au regard du cycle de vie des renseignements propres au service infonuagique et des exigences de PRP déclinées sous la forme d'objectifs, de pratiques, de sous-pratiques et de biens livrables.
- ✓ Détermination des principales mesures de PRP administratives, opérationnelles et technologiques qui seront mises en place pour atténuer ces risques et assurer le respect des exigences de PRP. Préciser en quoi ces mesures sont suffisantes pour réduire l'exposition aux risques à un niveau

19. Il importe de garder à l'esprit qu'une analyse de risques de sécurité, y compris des risques de sécurité juridique selon la Loi concernant le cadre juridique des technologies de l'information, ne couvre pas l'ensemble des exigences de PRP.

20. Se référer à Aide-mémoire pour faciliter l'intégration de la protection des renseignements personnels et la prise en compte des risques qui y sont associés lors du recours à des services infonuagiques, septembre 2014, disponible sur le site Web du Secrétariat à l'accès à l'information et à la réforme des institutions démocratiques dans la section « Outils » : http://www.institutions-democratiques.gouv.qc.ca/acces-information/documents/aide-memoire-infonuagique.pdf.

21. Considérer notamment les restrictions à l'accès (obligatoires ou facultatives) de la section II de la Loi sur l'accès. La communication d'un document « peut » ou « doit » dans certains cas être refusée par un organisme public lorsque cela a une incidence sur les relations intergouvernementales, sur les négociations entre organismes publics, sur l'économie, sur l'administration de la justice, sur la sécurité publique, sur les décisions administratives ou politiques, ou sur la vérification.

acceptable pour l'administration publique et fournir une assurance objective que la solution d'affaires développée est conforme aux exigences légales de PRP.

- ✓ Considération des risques particuliers liés à la localisation des données, notamment :
  - Évaluer les incidences que des informations soient localisées dans des organisations soumises à une ou des juridictions différentes : interceptions légales ou gestion contractuelle;
  - Évaluer les conséquences juridiques que les informations soient accessibles à d'autres entités gouvernementales ou entreprises;
  - Définir les conditions d'accès à l'information par une autre entité gouvernementale ou une entreprise;
  - Indiquer comment se fera le partage des responsabilités entre les différentes parties prenantes à l'égard de la mise en œuvre et du suivi des mesures de PRP associées au projet.
- ✓ Détermination des moyens visant à assurer la gestion des demandes d'accès aux documents et aux renseignements personnels, y compris la rectification de ceux-ci par des citoyens selon les exigences de la Loi sur l'accès :
  - Déterminer les règles d'accès aux documents à appliquer par le prestataire;
  - Élaborer des règles de gestion de l'exercice du droit d'accès aux renseignements personnels par la personne concernée et de rectification de ceux-ci à appliquer par le prestataire;
  - Obtenir un droit d'investigation en cas de non-respect des exigences de PRP par le prestataire de services.
- ✓ Détermination des mesures de gestion des renseignements personnels à mettre en place et à respecter par le prestataire de même que les obligations et les engagements des clients et des partenaires.
- ✓ Planification de la réalisation des mesures à mettre en place :
  - Déterminer les rôles et responsabilités des parties prenantes de l'organisation et du fournisseur et des ressources requises, notamment par la désignation d'une personne chez le fournisseur qui est responsable de la mise en application et du respect des exigences contractuelles à l'égard de l'accès, de la PRP et de la sécurité de l'information dans l'infonuagique, et d'en rendre compte;
  - Assigner les autres responsabilités et assurer la formation, le cas échéant;
  - Suivre et contrôler la réalisation des mesures de PRP et de sécurité ainsi que la qualité des processus à cet égard.
- ✓ Obtention d'un droit d'investigation en cas de non-respect des exigences de PRP par le prestataire.
- ✓ Harmonisation des travaux avec les personnes responsables de la gestion contractuelle et validation juridique (se référer au document «Volume 4 - Considérations en gestion contractuelle).
- ✓ Documentation et évaluation objective du processus de PRP réalisé (organisation et prestataire).
- ✓ Audit, par un tiers compétent et indépendant, de la qualité du processus de PRP réalisé et du respect des obligations en matière d'accès à l'information et de protection des renseignements personnels ou autrement confidentiels (déterminer si cela doit être intégré dans les exigences contractuelles).

2.4.4 L'hébergement des renseignements

L'externalisation des données propres à certains modèles de services infonuagiques, tels que le modèle public, suppose que certaines parties ou étapes du traitement des données pourraient se dérouler dans différents lieux et sous différentes juridictions. La division et la fragmentation que subissent les données au cours de cet hébergement peuvent rendre parfois difficile la localisation des données à un moment précis et dans une juridiction précise. Il pourrait donc s'avérer ardu, voire parfois impossible de déterminer le droit applicable. L'OP devrait alors s'informer auprès du prestataire de services des lieux où il entend héberger les données et circonscrire leur protection et leur sécurité dans le cadre contractuel. Toutefois, il faut le rappeler, aucun contrat, aussi bien rédigé soit-il, n'a préséance sur les lois d'un pays.

Lorsqu'il s'agit de renseignements personnels, une obligation supplémentaire s'impose aux OP. La Loi sur l'accès prévoit en effet que l'OP doit, avant de communiquer à l'extérieur du Québec de tels renseignements, ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, s'assurer qu'ils bénéficieront d'une protection équivalente à celle prévue à cette loi. Bien que cette mesure de la Loi sur l'accès ne touche que les renseignements personnels, celle-ci prévoit également des obligations de confidentialité pour des renseignements autres que personnels, et ainsi il pourrait être de bonne pratique d'étendre aussi cette exigence de protection aux renseignements dits autrement confidentiels.

Ainsi, si l'OP estime que ces renseignements ne bénéficient pas d'une protection équivalente à celle prévue à la Loi sur l'accès (ou à d'autres lois nécessitant que la confidentialité de certains renseignements soit assurée, selon la pratique proposée), il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte. Cette exigence prévue à la Loi sur l'accès devrait inclure tout lieu d'hébergement des renseignements personnels ou autrement confidentiels dont notamment les sites de relève. Il serait également important de préciser qu'elle s'étend aux sous-contractants du prestataire de services, le cas échéant.

Pour que l'OP puisse fournir l'autorisation d'héberger des renseignements à l'extérieur du Québec, le prestataire de services devrait soumettre pour examen les lois, règlements, procédures, standards, directives, politiques ou documents de même nature, de la province ou du pays où il détiendra les renseignements, les utilisera ou les communiquera. Il serait encore une fois de bonne pratique que le prestataire de services obtienne de l'OP l'autorisation d'héberger les renseignements à l'extérieur du Québec préalablement à la conclusion du contrat, ou dans le cas nécessitant le lancement d'un appel d'offres, avant la date de clôture de cet appel d'offres. Dans ce dernier cas, si l'autorisation d'héberger des renseignements à l'extérieur du Québec n'est pas accordée par l'OP, ceci éviterait au prestataire la préparation et l'élaboration d'une soumission parfois fastidieuse.

Les renseignements hébergés dans un autre pays sont soumis aux lois de ce pays, et il faut savoir qu'il est possible que ces dernières ne garantissent pas toujours leur disponibilité, leur intégrité et leur confidentialité ainsi que les obligations de PRP équivalentes à la Loi sur l'accès. Il serait donc important pour l'OP de comprendre le régime juridique applicable à la protection des renseignements et dans quelles circonstances des tribunaux, des organismes gouvernementaux ou encore des autorités de police d'autres pays pourraient y avoir accès.

À titre d'exemple, certaines lois telles que celle adoptée en 2001 par les États-Unis à la suite des attentats du 11 septembre, et plus connue sous le nom de USA PATRIOT Act[22], permettent notamment que les entreprises américaines, fournissant des services infonuagiques, quel que soit le lieu où elles font des affaires dans le monde, se soumettent aux demandes d'accès aux renseignements des autorités américaines dès lors qu'elles tombent sous le coup des lois américaines. En effet, les FISA (*Foreign Intelligence Surveillance Amendments*) permettent aux services de renseignements américains de s'affranchir des lois nationales pour accéder à des renseignements de citoyens non-américains sans

22. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USA PATRIOT Act) Act of 2001 (H.R. 3162).

aucune obligation de transparence à l'égard des États concernés. Ces entreprises sont tenues de satisfaire à ces requêtes, et ce, même si cela signifie de contrevenir aux lois auxquelles elles sont également soumises du fait de leurs activités sur un territoire donné.

Enfin, il est important de soulever le fait que certaines lois, notamment européennes[23], imposent aux OP qui soumettent leurs renseignements à des entreprises les hébergeant sur leur sol, des conditions et règles de sécurité entourant ces renseignements dont l'organisation devrait prendre connaissance. Ce faisant, l'OP pourrait décider de ne pas vouloir héberger ses renseignements dans certains territoires. Si l'OP décide de procéder ainsi, il verra à ne pas enfreindre les accords de commerce intergouvernementaux auxquels il est soumis, le cas échéant, ou, encore à ce que des dispositions dérogatoires de ces mêmes accords lui permettent d'agir de la sorte.

2.5 L'obligation d'assurer la sécurité de l'information

L'OP qui désire héberger des données dans le nuage devra s'assurer de mettre en place des mesures de sécurité spécifiques pour limiter les risques qui y sont associés. Pour ce faire, il devra prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la fiabilité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Dès qu'il est admis que certains documents technologiques voués à être hébergés dans le nuage nécessitent que l'on en assure la sécurité, il importe d'établir comment cette obligation doit être traduite juridiquement, et ce, même si les renseignements sont confiés à un tiers[24]. Pour ce faire, l'OP doit assurer la disponibilité des documents technologiques, leur intégrité et leur confidentialité[25].

Le principe de la disponibilité implique que les documents détenus par un OP se doivent d'être accessibles dans les délais convenables pour les personnes autorisées à en disposer dès qu'elles le désirent. Ces documents auront soit un caractère public, soit un caractère privé. Dans ce dernier cas, la disponibilité devra être contrôlée tant en ce qui a trait aux accès autorisés qu'en ce qui concerne le cycle de vie des documents.

Quant à l'intégrité des documents, elle doit être maintenue tout au cours de leur cycle de vie. En l'espèce, l'intégrité est assurée « lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue[26] ». Comme les documents technologiques versés dans le nuage sont conservés par le prestataire d'infonuagique, c'est à ce dernier que reviendra l'obligation d'assurer le maintien de l'intégrité des informations qu'ils contiennent[27]. Puisque cette conservation lui aura été déléguée par l'OP, celui-ci sera ultimement responsable des dommages causés par une conservation lacunaire[28].

Finalement, la confidentialité se définit comme étant la propriété d'un document dont l'information ne peut être divulguée à une personne non autorisée[29]. Cette notion vise certains types de renseignements personnels ainsi que d'autres renseignements qui, bien que normalement publics, pourraient être jugés confidentiels selon le contexte de leur collecte ou de leur conservation. Également, la notion de confidentialité peut être associée à celle du secret professionnel. Ainsi, lorsqu'un document technologique

23. *Data protection Act*, 1988, Irlande, http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html.
24. Nicolas VERMEYS, Julie M. GAUTHIER, et Sarit MIZRAHI, Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement du Québec, p. 79.
25. Loi concernant le cadre juridique des technologies de l'information, RLRQ, chapitre C-1.1.
26. Loi concernant le cadre juridique des technologies de l'information, RLRQ, chapitre C-1.1.
27. Nicolas VERMEYS, Julie M. GAUTHIER, et Sarit MIZRAHI, op. cit., p. 86.
28. Idem, note 6.
29. Nicolas VERMEYS, Julie M. GAUTHIER, et Sarit MIZRAHI, op. cit., p. 89..

contiendra un renseignement considéré comme confidentiel, l'entité responsable de sa détention devra prendre les mesures de sécurité propres à en assurer la confidentialité[30].

2.6 L'obligation de conservation et de préservation des documents

En vertu de la Loi sur les archives[31], il est prévu que tout OP doit établir et tenir à jour un calendrier de conservation qui détermine les périodes d'utilisation et les supports de conservation de ses documents actifs et semi-actifs. Ce calendrier indique quels documents inactifs sont conservés de manière permanente et lesquels sont éliminés. Tout projet de services infonuagiques devra bien entendu tenir compte de ces obligations et voir à ce qu'elles soient respectées, de même que toutes les autres obligations en découlant.

30. Cette section est basée sur le document suivant : Gouvernement du Québec : Denyse ROUSSEL et Denis BISTODEAU, Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics, 2009, version 1,1. En ligne , http://www.institutions-democratiques.gouv.qc.ca/acces-information/documents/modele-pratique-prp-2009.pdf.

31. Loi sur les archives, RLRQ, chapitre A-21.1.

Références

Aide-mémoire pour faciliter l'intégration de la protection des renseignements personnels et la prise en compte des risques qui y sont associés lors du recours à des services infonuagiques, http://www.institutions-democratiques.gouv.qc.ca/acces-information/documents/aide-memoire-infonuagique.pdf

Cadre de gestion et de valorisation de la propriété intellectuelle, http://www.mesrst.gouv.qc.ca/fileadmin/contenu/publications/RST/dispositions.pdf.

Code de procédure civile, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_25/C25.HTM

Data protection Act, 1988, Irlande, http://www.irishstatutebook.ie/1988/en/act/pub/0025/index.html.

Étude sur les incidences juridiques de l'utilisation de l'infonuagique par le gouvernement québécois (Nicolas VERMEYS, Julie M. GAUTHIER et Sarit MIZRAHI), (Université Laval), http://www.institutions-democratiques.gouv.qc.ca/acces-information/documentation.htm

Gazette officielle du Québec, 25 octobre 2000, 132e année, n°43, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=11&file=TMF0043.PDF

Loi concernant le cadre juridique des technologies de l'information, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_1_1/C1_1.html

Loi facilitant le paiement des pensions alimentaires, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_2_2/P2_2.HTM

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/G_1_03/G1_03.html

Loi sur la protection de la jeunesse, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/P_34_1/P34_1.html

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_2_1/A2_1.html

Loi sur l'administration fiscale, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=//A_6_002/A6_002.htm

Loi sur les archives, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/A_21_1/A21_1.htm

Loi sur les chemins de fer, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/C_14_1/C14_1.html

Loi sur les services de santé et les services sociaux, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=2&file=/S_4_2/S4_2.html

Modèle de pratiques de protection des renseignements personnels dans le contexte du développement des systèmes d'information par les organismes publics, 2009, version 1,1, http://www.institutions-democratiques.gouv.qc.ca/acces-information/documents/modele-pratique-prp-2009.pdf.

Recueil des politiques de gestion, http://www2.publicationsduquebec.gouv.qc.ca/home.php

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=3&file=/A_2_1/A2_1R2.HTM

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm

Secrétariat
du Conseil du trésor
Québec

Au cœur de l'administration publique