ISACA®
Section de Québec

Mémoire relatif au projet de loi 14 favorisant la transformation numérique de l'administration publique

Présenté à la Commission des finances publiques de l'Assemblée nationale du Québec

Présenté par David Henrard, président d'ISACA-Québec
Le 15 mai 2019

À propos d'ISACA

L'ISACA® (isaca.org), qui célèbre cette année son 50e anniversaire, est une association mondiale qui aide les particuliers et les entreprises à tirer profit du potentiel positif de la technologie. Le monde d'aujourd'hui est alimenté par l'information et la technologie, et l'ISACA fournit aux professionnels les connaissances, les titres de compétences, l'éducation et la communauté nécessaires pour faire progresser leur carrière et transformer leur organisation.

L'ISACA tire parti de l'expertise de ses 460 000 professionnels engagés dans les domaines de l'information et de la cybersécurité, de la gouvernance, de l'assurance, du risque et de l'innovation, ainsi que de sa filiale CMMI® Institute, axée sur la performance des entreprises, pour faire progresser l'innovation par la technologie. L'ISACA est présent dans 188 pays, dont plus de 220 sections dans le monde entier et des bureaux aux États-Unis et en Chine.

Faits et chiffres sur ISACA

Créé en : 1969
Professionnels engagés: 460.000
Membres: 140.000 dans 188 pays
Nombre de membres et de détenteurs de certification : 166.000
Chapitres: Plus de 220
Groupes d'étudiants: 97

Les certifications d'ISACA

L'ISACA a élaboré et administre des certifications à la fine pointe de l'industrie :

Certified Information Systems Auditor® (CISA®). Plus de 146.000 certifiés depuis sa création en 1978.

Certified Information Security Manager® (CISM®). Plus de 43.000 certifiés depuis 2002.

Certified in Risk and Information Systems Control™(CRISC™). Plus de 25.000 certifiés depuis 2010.

Certified in the Governance of Enterprise IT® (CGEIT®). Plus de 8.000 certifiés depuis 2007.

CSX Practitioner Certification (CSXP™) est une certification basée sur la performance qui permet aux praticiens de valider leurs compétences en tant que premiers intervenants en cybersécurité. L'examen de certification des praticiens de la CSX (CSXP) a été amélioré en 2018 pour tenir compte des tâches et des défis actuels en matière de cybersécurité et pour permettre une administration souple et à distance.

Les produits et services d'ISACA

L'ISACA fournit une multitude d'outils et de ressources aux professionnels des technologies d'affaires et à leurs entreprises :

ISACA s'associe à des individus et à des organisations pour faire en sorte qu'évoluent dans le monde, la situation, les informations prêtes à l'emploi et la main d'œuvre en cybersécurité. La plate-forme Cebersecurity Nexus (CSX), https://cybersecurity.isaca.org fournit des modules de formations, des outils d'évaluation basés sur la performance, des études, un réseau, des conférences et des contenus. Elle inclut le CSX Training Platform; Cybersecurity Fundamentals certificate, CSX Practitioner certification et la NEXUS e-newsletter.

L'ISACA guide les leaders sur la façon de gouverner efficacement les systèmes d'information d'aujourd'hui et les technologies émergentes de demain. COBIT® est le cadre de référence pour la gouvernance et la gestion de l'information de l'entreprise et des technologies depuis plus de 20 ans.

En 2016, l'ISACA a acquis le CMMI Institute de l'Université Carnegie Mellon. Les évaluations CMMI permettent aux entreprises de mesurer leur capacité et leur maturité par rapport à un cadre défini de meilleures pratiques et d'identifier de manière décisive les domaines dans lesquels elles doivent être plus compétitives. La plate-forme CMMI Cybermaturity Platform, une plate-forme complète d'évaluation des risques et des capacités de cybersécurité d'entreprise qui fournit aux responsables de la cybersécurité et aux cadres supérieurs les preuves et les connaissances nécessaires pour améliorer la résilience de la cybersécurité.

À propos d'ISACA Québec

Créée en 1984, ISACA-Québec (isaca-quebec.ca) propose à ses 200 membres, à la communauté des professionnels de la grande région de Québec et à la communauté universitaire un programme annuel de conférences, des activités de formation et de multiples occasions de réseautage.

Elle s'implique régulièrement auprès des étudiants pour susciter des vocations dans des domaines touchés particulièrement par la pénurie de mains d'œuvre alors même que les organisations des secteurs publics et privés sont confrontées aux enjeux de la transformation numérique, à des risques croissants en matière de cybersécurité et de risques découlant de technologies émergentes.

L'équipe de bénévoles qui composent ISACA-Québec s'est investie afin de traduire en français le référentiel COBIT®5, référentiel orienté affaires sur la gouvernance et la gestion de l'information et des technologies de l'entreprise.

Ces efforts se sont traduits par l'adoption de COBIT®5 comme outil de référence par différents organismes publics tels que le Vérificateur général du Québec, la Caisse de dépôt et placement du Québec, Revenu Québec, la SAAQ ainsi que la Ville de Québec et la Ville de Montréal.

Toutes ces réalisations sont le fruit de bénévoles et ont valu à ISACA-Québec d'être, à de nombreuses reprises, primée par ISACA International au cours de ses 35 ans d'activité.

ISACA®
Section de Québec

Exposé général

Mise en contexte :

Aujourd'hui, toutes les organisations à travers le monde, qu'elles soient publiques ou privées font face aux défis de la technologie et doivent considérer leur transformation numérique pour plusieurs raisons qu'il s'agisse :

- Du désir d'améliorer la performance de leur organisation
- De la volonté d'offrir des produits et services innovants et toujours plus adaptés
- D'une demande d'une clientèle désormais hyperconnectée et avide de simplicité et de rapidité
- D'un souci environnemental de limiter le recours aux supports papier

Cependant, cette transformation numérique apporte son lot de défis :

- La maitrise des projets visant à réaliser cette transformation numérique
- La sécurité de l'information et tout particulièrement la cybersécurité qui est au cœur de cette transformation
- La protection de la vie privée des personnes dont les renseignements personnels seront utilisés dans les systèmes d'information

Discussion relative au projet de loi 14

De manière générale si nous saluons la volonté du gouvernement de permettre à l'administration publique de tirer profit de l'information et des technologies par sa transformation numérique, nous éprouvons un certain malaise avec le manque de précision du projet de loi 14 dans sa forme actuelle.

En effet, la transformation numérique peut prendre différentes formes et donner lieu à bien des initiatives.

Cependant, en dehors des informations dont nous avons pu prendre connaissance dans les médias, le projet de loi reste très générique quant à la nature des projets qui vont voir le jour.

La notion de projet en ressources informationnelles désigné d'intérêt gouvernemental dont il est fait mention n'est pas définie et les critères associés à un tel projet ne sont pas précisés.

L'essentiel du projet porte sur la communication et l'utilisation de renseignements personnels et une autorisation qui serait faite au gouvernement de s'affranchir de dispositions incompatibles de loi existantes.

Or ces actuels éléments bloquants ne sont pas exposés, la nature des renseignements personnels visés n'est pas précisée et les acteurs (organisme public détenant les renseignements personnels et la personne ou l'organisation qui en recevrait la communication pour les utiliser) ne sont pas identifiés.

Nous comprenons que la loi ne peut pas entrer dans un niveau de détail élevé, mais compte tenu de la nature des risques qui pourront peser sur ces renseignements et donc a fortiori sur les personnes concernées par ces renseignements, quelques précisions quant à la nature des contrôles qui seront mis en place pourraient être insérées au projet de loi.

Cela est d'autant plus important à nos yeux que la confiance du citoyen est essentielle dans un contexte où la confidentialité des renseignements personnels est de plus en plus mise à mal et alors que les législateurs de différents pays, notamment au niveau de l'Union européenne, renforcent leur arsenal législatif.

À titre d'information, le Commissariat à la protection de la vie privée du Canada vient de publier, le 9 mai 2019, les résultats d'un sondage[1] démontrant que les Canadiens se préoccupent de leur vie privée en ligne et veulent exercer plus de contrôle sur leurs renseignements personnels.

Ce sondage mentionne notamment que 64 % des personnes interrogées ne souhaitent pas que les ministères communiquent leurs renseignements à un autre ministère sans leur consentement.

Ainsi, nous accueillons favorablement les dispositions du projet de loi relatives au rôle de contrôle qui sera exercé pas la Commission d'Accès à l'information même s'il n'est pas précisé ce qu'il adviendra en cas d'avis défavorable.

Les rôles et les responsabilités des différents intervenants en matière de protection des renseignements personnels pourraient également être précisés notamment en cas de violation de confidentialité.

De manière générale, il est vrai que la transformation numérique passe le plus souvent par un accroissement de la circulation des données.

L'utilisation des renseignements personnels des citoyens pourrait permettre aux organismes publics de mieux connaitre le profil des utilisateurs des services et d'évaluer la performance des programmes et permettre au gouvernement de prendre des décisions sur la base d'informations précieuses.

Une telle utilisation statistique des données peut cependant se faire dans la plupart des cas en ayant recours au mécanisme d'anonymisation des données voire de dépersonnalisation. Selon le contexte, il peut s'agir d'un mécanisme complexe, mais qui a le mérite de diminuer grandement le risque d'atteinte à la vie privée des personnes concernées notamment en évitant la propagation de ces renseignements en autant de systèmes qu'il faudra alors sécuriser.

Cette disposition pourrait prendre la forme de l'insertion dans le projet de loi 14 d'un principe de précaution visant à prioriser le recours à la communication de données anonymisées plutôt que de renseignements personnels.

Un aspect de la transformation numérique de l'administration publique concerne l'accès simplifié aux services en ligne du gouvernement du Québec. Pour permettre cet accès,

[1] https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2019/nr-c_190509/

une initiative nommée « Accès UniQc » est en préparation. D'autres gouvernements ont été confrontés à ce besoin et des solutions ont vu le jour[2]. Cependant ces solutions reposent sur un mode de fonctionnement qui limite au maximum le partage d'information entre les différentes organisations participantes[3]. Ainsi le gouvernement fédéral du Canada a mis en place une solution permettant aux citoyens d'accéder aux sites de 24 entités gouvernementales en s'appuyant sur des identités propres à chacune de ces organisations, mais avec un moyen d'authentification commun (authentification gouvernementale ou bancaire) et permettant de garantir la protection de la vie privée des citoyens. Il est à noter que c'est le modèle retenu par l'Agence du revenu du Québec.

Ce faisant, le gouvernement se met à l'abri de la création d'un point unique qui, s'il devait comporter des vulnérabilités, serait une cible de choix pour des cyberattaques.

Enfin, nous souhaiterions vous faire part de notre questionnement quant à la l'emploi de la notion de « projet en ressources informationnelles d'intérêt gouvernemental ».

Selon notre compréhension, cela exclut l'exploitation et l'utilisation de l'actif informationnel ou du service en ressources informationnelles émanant du projet. Or c'est à ce moment-là, selon nous, que la nécessité de disposer de l'information ou des renseignements personnels se manifeste.

Une clarification s'impose, car le projet de loi 14 n'aborde pas la question importante du devenir, au terme du projet, des renseignements personnels utilisés et communiqués.

[2] Afin d'aider la communauté à profiter de ces expériences, ISACA-Québec organisera du 7 au 9 octobre 2019 à Québec un congrès international sur les technologies émergentes et une journée entière y sera consacrée sur la façon de gérer les identités numériques – voir www.isaca-quebec-2019.org – Y seront notamment présentés les principes du « Digital ID & Authentication Council of Canada » en matière de gestion de l'identité numérique : https://diacc.ca/principles/

Analyse article par article du projet de loi 14

Article 1

Notre compréhension est que l'alinéa 2 de l'article 1 énonce un principe de respect du droit à la vie privée, de transparence et de promotion de la confiance.

Cependant, dans sa forme actuelle, nous estimons que le projet de loi 14 ne respecte que partiellement ce principe. Nos commentaires sur les autres articles du projet de loi appuient cette impression.

Article 2

La notion de projet en ressources informationnelles fait référence à « un ensemble d'actions menant au développement, à l'acquisition, à l'évolution ou au remplacement d'un actif informationnel ou d'un service en ressources informationnelles »[4].

Notre compréhension de la notion de projet est que cet ensemble d'actions a un début, mais également une fin qui n'inclut pas l'exploitation de l'actif ou du service visé.

Ainsi, l'utilisation des renseignements personnels et les communications n'interviendraient que dans le cadre de ce projet et non pour permettre l'exploitation de l'actif ou du service en question?

Article 3

Cet article prévoit l'utilisation et la communication des renseignements personnels à toute personne ou à tout organisme (…)

Cette notion de personne vise-t-elle les personnes physiques et les personnes morales? À défaut, il serait utile de le préciser. En pratique, de qui peut-il s'agir?

De la même manière, quand il est question d'organisme, cet organisme est-il un organisme public ou peut-il également s'agir d'un organisme privé? Le cas échéant, quels exemples d'organisations sont visés?

Concernant les renseignements personnels concernés, peut-il s'agir de n'importe quel type de renseignements? Par exemple pourrait-il s'agir de renseignements contenus dans le dossier d'un citoyen? Les médias ayant mentionné le nom du programme « Accès UniQc », ne serait-il pas prudent, dans ce cas, de limiter les renseignements personnels visés aux renseignements personnels permettant l'identification du citoyen?

L'article 3 limite l'utilisation des renseignements personnels et leur communication aux cas où ils seraient « nécessaires à la réalisation d'un projet en ressources informationnelles d'intérêt gouvernemental. » En utilisant cette notion de projet (voir

[4] Article 16.3 de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement.

notre commentaire à l'article 2) cela limite l'utilisation et la communication aux activités du projet. Ne faudrait-il pas utiliser une autre notion telle que « nécessaire au fonctionnement d'un service ». Cela poserait peut-être néanmoins une difficulté quant à la définition de ce que serait un service « d'intérêt gouvernemental ».

Outre le fait que l'utilisation et la communication des renseignements personnels dans le cadre d'un projet est limitatif pour l'exploitation du service qui en résultera, cela soulève une question importante relative à la protection de la vie privée. En effet, toutes les bonnes pratiques en matière de projet recommandent de ne pas utiliser de renseignements personnels dans des projets, mais plutôt d'utiliser des données anonymisées ou dépersonnalisées.

Cette règle s'explique par le fait que les projets, notamment les projets de développement de solutions informatiques, se déroulent dans des environnements technologiques autres que les environnements de production. Or ces environnements ne bénéficient pas du même niveau de protection que la production.

De plus, les personnes agissant dans le cadre d'un projet n'ont généralement pas la qualité (au sens de la loi sur l'accès) pour accéder à ces renseignements personnels.

À propos de l'alinéa 3 de l'article 3, nous comprenons que conformément à l'alinéa 2 de l'article 1, aucun décret pris en application de cette loi ne pourra aller à l'encontre du principe de respect du droit à la vie privée. Il découle alors de ce principe le fait que le citoyen devrait disposer d'un droit à l'information préalable à l'usage et à la communication de ses renseignements personnels ainsi que d'un droit à y consentir ou pas.

L'alinéa 4 de l'article 3 qui est au cœur du projet de loi prévoit que cet article « s'applique malgré toute disposition inconciliable d'une loi… ».

Nous nous interrogeons sur la portée de cette disposition. Vise-t-elle n'importe quelle loi et notamment peut-il s'agir de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels?

Dans l'affirmative, le projet de loi 14 n'enverrait-il pas un signal contradictoire avec l'alinéa 2 de l'article 1 réaffirmant le principe du respect du droit à la vie privée.

En limitant l'application de cette loi, le Québec ne s'exposerait-il pas à des conséquences en matière d'équivalence requise par la loi fédérale pour permettre aux provinces de légiférer en matière de protection des renseignements personnels?

L'alinéa 2 de l'article 3 mentionne la possibilité de confier à un organisme public toute fonction ou toute responsabilité liée à la réalisation d'un tel projet. Encore là, notre compréhension de la notion de projet nous amène à penser que cela ne pourra se faire que durant la réalisation d'un projet et non au-delà de son terme.

Pour faciliter notre compréhension, a-t-on à ce stade des exemples de telles fonctions ou responsabilités qui pourraient être confiées à un organisme public?

Article 4

Sans revenir sur la notion de personne ou d'organisme abordée à l'article précédent et des bonnes pratiques de non-utilisation des renseignements personnels dans le cadre d'un projet, nous comprenons que l'utilisation des renseignements personnels sera limitée « aux fins de la réalisation du projet ». Ainsi libellé, nous comprenons que le projet de loi 14 ne vise pas les situations postérieures à la clôture du projet et notamment l'utilisation de renseignements personnels dans le cadre du fonctionnement du système ou du service qui aura été créé par le projet.

Nous prenons note avec satisfaction que la personne ou l'organisme visé ne pourra pas communiquer à son tour de tels renseignements.

Concernant l'obligation qui lui est faite de prendre les mesures de sécurité propres à assurer leur protection, le projet de loi ne précise pas les différents rôles et responsabilités. L'organisme public d'origine disposera-t-il par exemple d'un droit de regard sur le choix et la mise en œuvre de ces mesures de sécurité? Quel rôle jouera par exemple le responsable de la protection des renseignements personnels de chacun des organismes?

Article 5

Cet article porte sur la possibilité de l'existence d'un « degré élevé d'attente raisonnable en matière de vie privée ». Nous comprenons que cette attente pourrait émaner du citoyen dont les renseignements sont visés lorsqu'il existe un risque important d'atteinte à sa vie privée. Comment en pratique le citoyen aura-t-il l'occasion de l'exprimer. Une consultation sera-t-elle prévue avant le démarrage d'un projet?

Article 6

Comme précédemment, notre compréhension est que les périodes visées sont de nature à correspondre à la durée du projet visé et donc ne vise pas l'exploitation du service ou du système qui aura été mis en place par le projet.

Article 7

La possibilité offerte à la Commission d'accès à l'information de donner son avis nous semble un minimum. Ne serait-il pas plus prudent d'avoir un avis systématique? Le gouvernement sera-t-il lié par l'avis de la CAI? Sans ces précisions et compte tenu des moyens dont dispose la CAI, nous craignons qu'elle ne soit pas en mesure de donner son avis et ainsi d'exercer sa mission de gardien de la protection de la vie privée des citoyens.

Article 8

L'article 8 introduit la notion d'organisme public responsable de la gestion d'un projet en ressources informationnelles d'intérêt gouvernemental. Cette notion doit-elle être comprise comme étant la même que la personne ou l'organisme à qui des renseignements personnels sont communiqués? À défaut, comment se fera l'interaction entre ces deux entités notamment en lien avec la protection de ces renseignements, incluant la reddition de compte?

Il est fait mention dans l'article d'une évaluation des facteurs relatifs à la vie privée à différentes étapes du projet. Nous comprenons qu'une telle évaluation devra être faite dès la conception, mise à jour lors de toute modification et au terme du projet.

L'article 8 prévoit également que l'organisme en question devra prendre toutes les mesures appropriées afin d'assurer la protection des renseignements personnels.

Parmi les mesures habituellement attachées à la protection des renseignements personnels figure l'obtention préalable du consentement de la personne concernée par les renseignements en question. Cette notion n'apparaissant pas dans le projet de loi 14, nous souhaiterions avoir confirmation qu'elle fera bien partie des mesures mises en place.

Ce consentement devant être obtenu préalablement à la communication des renseignements personnels pourrait nécessiter de faire l'objet d'une disposition explicite dans le projet de loi.

L'alinéa 2 de l'article 8 prévoit la diffusion sur le site Internet de l'organisme public responsable de la gestion du projet d'une copie de l'évaluation des facteurs relatifs à la vie privée. Cette mesure est de nature à contribuer à la transparence vis-à-vis du citoyen. Cependant il est à noter que ce type d'évaluation peut comporter des informations sensibles telles que des détails techniques pouvant être utilisés par des personnes malveillantes. Il serait opportun de prévoir la publication d'un résumé plutôt que l'évaluation intégrale, comme cela est préconisé au niveau fédéral.[5]

Concernant cette publication, s'agira-t-il de l'unique moyen utilisé pour assurer la transparence envers les citoyens?

Article 9

Cet article portant sur différentes mesures de reddition de compte aborde la question de la clôture du projet. Comme mentionné lors de notre commentaire de l'article 2, cette notion de projet se réfère en effet à une séquence qui a une fin. Or, le projet de loi ne précise d'aucune manière ce qu'il advient des renseignements personnels utilisés et communiqués lors de ce projet. Qu'adviendra-t-il? Devront-ils être détruits?

[5] Directive sur l'évaluation des facteurs relatifs à la vie privée du SCT – Gouvernement du Canada

Article 10

Nous comprenons que ce projet de loi créerait un régime temporaire. Cette limitation dans le temps nous semble une bonne chose pourvu qu'une révision de la loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels finisse par intervenir. Que se passera-t-il néanmoins si l'un des projets visés devait ne pas être terminé à cette date?

Articles 11

Pas de commentaire.

Article 12

Pas de commentaire.