Projet de règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique

Mémoire présenté au Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité

Par les étudiants du cours BIM717 et DRT871
dirigé par Me Antoine Guilmain

Septembre 2023

* Me Antoine Guilmain, LL.D., est chargé de cours à la Faculté de droit de l'Université de Sherbrooke et cochef du groupe de pratique national Cybersécurité et protection des données chez Gowling WLG.
Coordonnées : antoine.guilmain@usherbrooke.ca

UdS Université de Sherbrooke

Sommaire

INTRODUCTION

Le présent mémoire est soumis suite à la présentation du *Projet de règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique*[1] (le « Projet de règlement ») découlant du nouvel article 63.4 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « *Loi sur l'accès* ») tel qu'amendé par la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (la « Loi 25 »).

Dans le cadre du cours BIM717 et DRT871 (*Données numériques et sciences de la vie*), les étudiants ont commenté le Projet de règlement à titre d'évaluation finale. Le présent mémoire vise à présenter sous forme agrégée les commentaires de la cohorte. D'abord, nous donnerons un aperçu général de l'appréciation des étudiants vis-à-vis du Projet de règlement. Par la suite, nous ferons ressortir les faits saillants, soit les principaux commentaires qui reviennent à la lecture des étudiants. Enfin, l'intégralité des commentaires est reproduite dans les pages dans un esprit de transparence et d'exhaustivité.

DESCRIPTION DU COURS

Le cours *Données numériques et sciences de la vie* (2e cycle, Faculté de droit de l'Université de Sherbrooke) vise à familiariser les étudiants avec le cadre normatif et éthique applicable aux données numériques dans le domaine des sciences de la vie. Il permet aussi aux étudiants de saisir les enjeux liés à la confidentialité, à la sécurité des données, aux technologies de l'information et aux nouveaux modèles d'affaires. Le contenu du cours est appliqué à des situations concrètes, souvent d'actualités, dans le but d'outiller les étudiants face à la législation locale et internationale visant les données numériques.

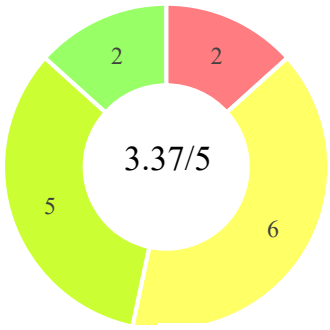
MODALITÉS D'ÉVALUATION

À titre d'évaluation finale, les étudiants ont commenté le Projet de règlement (reproduit en Annexe 2) en vue d'appliquer les notions acquises lors du cours. Cette évaluation prenait la forme d'un questionnaire divisé en deux parties (reproduit en Annexe 1). D'une part, les étudiants ont décrit leur appréciation globale du Projet de règlement et des enjeux qui en ressortent. D'autre part, les étudiants ont fourni des commentaires spécifiques visant les dispositions du Projet de règlement.

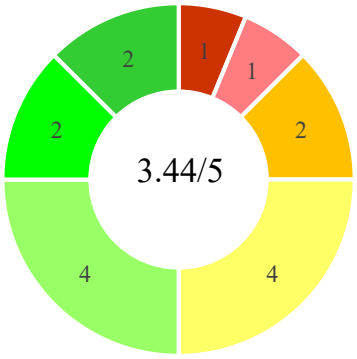
[1] Gazette No. 28 du 12-07-2023, page : 3246

APERÇU GÉNÉRAL SELON LES ÉTUDIANTS

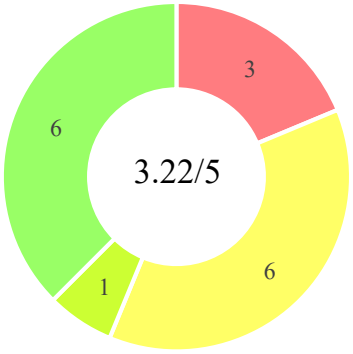
Évaluation générale du Projet de règlement



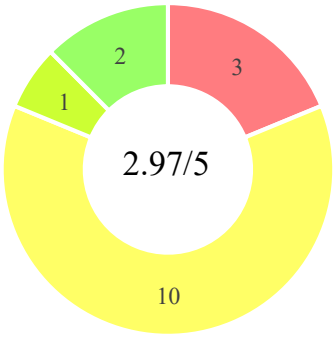
Validité juridique du projet de règlement



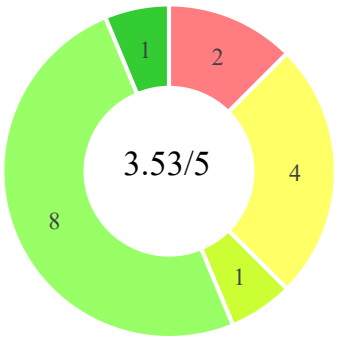
Portée adéquate du projet de règlement



Application concrète du projet de règlement



Format et clarté du projet de règlement



Légende : 1/5 1,5 /5 2/5 2,5/5 3/5 3,5/5 4/5 4,5/5 5/5

*Les 16 étudiants répondants ont tenté d'évaluer leur appréciation pour certains aspects fondamentaux du Projet de règlement. À cet effet, voir les questions générales du questionnaire reproduit à l'Annexe 1.

FAITS SAILLANTS

- En général, le Projet de règlement présente des propositions intéressantes pour le public, surtout, dans la mesure où nous souhaitons voir une meilleure harmonisation du contenu des politiques de confidentialité au Québec. Il s'agit d'une manifestation claire de l'importance accordée à la transparence, au profit d'un consentement plus libre et éclairé des individus envers toute organisation traitant des renseignements personnels.

- Les conditions de forme et de fond liées aux politiques de confidentialité témoignent de la qualité qui est attendue de celles-ci, consolidant l'engagement du législateur québécois au profit d'une meilleure protection des renseignements personnels des citoyens. Autrement dit, selon les étudiants, il s'agit certainement « d'un pas dans la bonne direction ».

- Toutefois, par l'exercice ci-joint, les répondants proposent quelques commentaires constructifs visant à renforcer le Projet de règlement au bénéfice des multiples parties prenantes, dont nous reproduisons les points principaux ici :

    1. *Élargir le champ d'application afin d'y réunir les organismes publics et le secteur privé sous un cadre réglementaire unique, à l'exclusion des PME, sauf celles qui traitent un volume substantiel ou sensible de renseignements personnels ;*
    2. *Nuancer le champ d'application en fonction de la quantité des renseignements personnels traités, ou encore eu égard à la sensibilité de ceux-ci ;*
    3. *Remplacer l'expression « politique de confidentialité » par une terminologie plus juste (« avis relatif à la protection des renseignements personnels ») ;*
    4. *Encadrer davantage le format et la structure d'une politique de confidentialité, en tenant compte du besoin de simplicité et en privilégiant l'approche par couche ;*
    5. *Exiger plus d'informations sur le cycle de vie des renseignements personnels, par une mention décrivant la durée de conservation des données et la gestion de fin de cycle ;*
    6. *Ajouter des conditions de suppression des renseignements personnels ;*
    7. *Prescrire une mention relative au consentement du mineur de moins de 14 ans, lequel doit être validé par un représentant légal ;*
    8. *Considérer une mention liée à la collecte de renseignements personnels par une technologie comprenant des fonctions d'identification, de localisation ou de profilage ;*
    9. *Détailler les modalités de la collecte commune de renseignements personnels par des organismes publics, notamment quant à la coordination des mesures de sécurité en place et à l'attribution de la responsabilité à cet égard ;*
    10. *Intégrer des exigences liées aux technologies de suivi pour resserrer l'encadrement relatif aux témoins de connexion ;*
    11. *Restreindre la portée des articles liés à l'avis de modification, afin de limiter la procédure aux modifications « substantielles » à la politique de confidentialité ; et*
    12. *Intégrer le principe de la neutralité technologique en permettant l'utilisation de tout moyen pour publiciser la politique auprès du public.*

COMMENTAIRES DÉTAILLÉS

1. QUESTIONS GÉNÉRALES

1.1 Quelle évaluation générale faites-vous du projet de règlement ?

Le projet de règlement aura, selon moi, des impacts positifs sur les pratiques de gestion des renseignements personnels des organismes publics récoltant ces renseignements par un moyen technologique. En effet, le projet de règlement s'articule autour des principes fondamentaux concernant les renseignements personnels, soit la transparence et le consentement. Il assurera aussi une meilleure uniformité ainsi qu'une harmonisation dans les pratiques des organismes. Toutefois, le fait que le projet de règlement ne s'applique qu'aux organismes publics récoltant les renseignements personnels par moyen technologique minimise les impacts positifs qu'il pourrait apporter s'il était applicable à tous les organismes publics et privés. À titre d'exemple, en Europe, avec le *Règlement général sur la protection des données* (ci-après « RGPD ») les entités du secteur public ainsi que du secteur privé sont assujetties aux mêmes obligations. Finalement, il aurait été pertinent que le projet de règlement adresse la problématique de l'accessibilité de l'information pour le public cible, en incluant des prescriptions, notamment quant au format, à la structure ou à la longueur du texte. En effet, l'accessibilité de l'information pour le lecteur est un élément essentiel du consentement de ce dernier. D'ailleurs, d'autres domaines de droit le reconnaissent, par exemple, le *Règlement d'application de la Loi sur la protection du consommateur* (RLRQ, c. P-40.1, r. 3) édicte des balises quant à la taille des caractères utilisés ou même aux couleurs utilisées. Il pourrait être pertinent que le projet de règlement le fasse aussi.	Le projet de règlement précise ce que doit minimalement contenir la politique de confidentialité, mais le projet de règlement n'encadre pas le format ni la structure de la politique de confidentialité. Comme mentionné à l'article 63.4 de la Loi sur l'accès, la politique de confidentialité doit être rédigée en termes simples et clairs. Celle-ci doit également être intelligible pour que toute personne puisse bien comprendre ses droits et la manière dont les renseignements personnels sont recueillis et utilisés. Il existe des formats ou des structures qui pourraient faciliter la lecture et la compréhension de la politique de confidentialité. Ainsi, je suggère que le projet de règlement exige que toute politique de confidentialité débute avec un bref résumé et que son contenu soit divisé en différentes sections déterminées dans le projet de règlement. À titre d'exemple, le projet de règlement pourrait imposer qu'une politique de confidentialité contienne les sections suivantes : collecte, utilisation et communication de renseignements personnels, droit des individus, sécurité, conservation et coordonnées. De plus, le projet de règlement ne tient pas suffisamment compte de la collecte de renseignements personnels par une technologie comprenant des fonctions permettant d'identifier, de localiser ou d'effectuer un profilage. Certaines exigences prévues dans le projet de règlement manquent de clarté et d'autres alourdissent inutilement le fardeau des organismes publics. Le projet de règlement manque aussi de cohérence avec sa loi habilitante.
Dans son ensemble, le règlement est très concis. En ce qui concerne son contenu, il est possible que certaines de ces dispositions suscitent de la confusion chez quelques organismes publics. En effet, la volonté de vouloir faire un règlement très bref peut parfois faire en sorte que certains articles nécessitent plus de précision afin de ne pas confondre l'intention du législateur et bien interpréter le règlement. Entre autres, certains articles comme les articles 4 et 5 peuvent mener, en pratique, à des difficultés potentielles puisqu'elles comportent des exigences trop lourdes, surtout compte tenu de l'évolution rapide de la technologie et du flou autour de la notion de « modification significative ». De plus, quelques éléments du projet de règlement démontrent des	Le projet de règlement impose des contraintes quant aux politiques de confidentialité, tel que sur leurs contenus, leurs publications et leurs modifications. Ce règlement devrait assurer que les différentes politiques de confidentialité des organismes gouvernementaux contiennent certaines informations minimales et soient relativement similaires. Le projet de règlement est écrit de manière très spécifique et précise, et laisse peu de place à interprétation. Par exemple, la liste de l'article 2 du projet est écrite de manière précise et donne toutes les informations nécessaires à mettre dans la politique de confidentialité. Le texte du projet de règlement permet d'aider dans la protection des citoyens quant à leur droit à la vie privée. En effet, en

incohérences avec les lois applicables, notamment avec la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Une fois que ces petites imperfections seront corrigées, le projet de règlement sera beaucoup plus clair et les politiques de confidentialité en découlant seront beaucoup plus adaptées aux personnes auxquelles elles sont destinées. Malgré tout, le règlement est quand même précis et détaille bien les éléments que devrait contenir une politique de confidentialité. Bien que le projet soit bien détaillé, certains ajouts pourraient être faits afin d'être plus précis et d'assurer une meilleure protection des renseignements personnels.	obligeant les organismes publics à avoir une politique de confidentialité, et en s'assurant que celles-ci soient rédigées de manière similaire, cela permettra au public d'avoir une meilleure compréhension des informations qu'il donne au gouvernement, et de la raison pour laquelle cela est nécessaire. Ainsi, je pense que le projet de règlement harmonisant les politiques de confidentialité permettra, indirectement que le public comprenne mieux leurs droits. En somme, le projet de règlement semble imposer des obligations particulièrement spécifiques aux organismes gouvernementaux, mais cela est nécessaire pour qu'il puisse atteindre son objectif. En effet, les termes précis et les listes d'obligations permettront de rédiger des politiques de confidentialité qui aideront le public à mieux comprendre leurs droits. Je considère donc que ce projet utilise les bonnes stratégies pour atteindre son objectif.
Mon opinion par rapport au projet de règlement est globalement positive. À mon avis, il atteint son objectif initial qui est d'augmenter la transparence des organisations en lien avec la collecte de données auprès des usagers. De plus, il clarifie l'application de l'article 63.4 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « *Loi sur l'accès* ») pour les organisations en leur offrant un cadre clair et précis. Néanmoins, j'ai relevé deux critiques générales sur ce projet de règlement. Premièrement, je trouve qu'il impose des restrictions trop importantes pour le secteur public. En effet, alors que les normes qu'il établit se veulent minimales, elles semblent pourtant très exigeantes. Je crois que le projet de règlement devrait plutôt miser sur des contraintes au niveau de la forme de la politique telle que le fait qu'elle doive être concise, bien structurée et qu'elle doive comprendre des schémas pour faciliter la lecture. Ma seconde critique est que le projet de règlement s'est en quelque sorte limité à clarifier l'article 63.4 de la *Loi sur l'accès* et en se faisant, il n'a pas suffisamment considéré les principes généraux entourant la vie privée telle que le consentement. Il aurait été notamment bénéfique d'inclure des dispositions sur les mécanismes de consentement à une politique de confidentialité, ainsi que sur les façons de retirer ce consentement. Par exemple, le projet de règlement aborde certains concepts tels que les *joint controllers*, mais n'énonce pas les implications de celui-ci pour l'usager.	Je crois qu'il s'agit d'un règlement qui apporte des précisions pertinentes quant au contenu d'une politique de confidentialité, mais qui comporte plusieurs lacunes importantes qui font en sorte que son applicabilité n'aura peut-être pas l'impact envisagé. La première faille est, selon moi, le champ d'application. Je trouve très particulier qu'il ne s'applique qu'aux organismes publics, bien que je comprenne que le règlement est édicté par l'entremise de l'article 63.4 de la Loi sur l'accès. D'après moi, les objectifs qu'on souhaite atteindre par ce règlement sont, ou devraient être, les mêmes pour le secteur privé, notamment lorsqu'il est question d'harmonisation du contenu des politiques de confidentialité. D'autant plus que l'hétérogénéité de ces politiques est souvent plus flagrante parmi les entreprises et constitue un réel obstacle pour les utilisateurs. En outre, je suis plutôt contente du fait que le Québec est assez rigide par rapport à la protection des renseignements personnels, puisque cela favorise du même coup la protection des droits des individus. Cependant, un tel niveau de rigidité exige de l'exhaustivité et de la cohérence et ce sont peut-être des notions manquantes dans ce projet. Par exemple, la politique, selon le règlement, n'a pas besoin d'aborder le retrait ou la conservation des renseignements (contrairement à la LPRPDE et au RGPD), alors qu'il s'agit d'un élément important qui est intrinsèquement lié au consentement. Également, je ne trouve pas que le concept de collecte commune est bien encadré.
De façon générale, le projet de règlement répond à son objectif premier, soit de déterminer le	Le projet de règlement présente des points forts, mais aussi des points faibles importants. Points

contenu et les modalités d'une politique de confidentialité et d'un avis de modification. Les termes utilisés sont généralement assez simples et clairs. Son contenu est donc relativement clair, tout comme son format. Les différentes sections du règlement en facilitent sa compréhension et font ressortir les éléments essentiels quant aux politiques et aux avis. Toutefois, considérant le fait qu'un tel projet de règlement ne doit pas être compris seulement par les spécialistes, mais également par tout citoyen, consommateur ou organisme moyen, certaines précisions devraient y être ajoutées. Pour ceux étant moins familiers avec la terminologie et les principes liés aux renseignements personnels, ce projet de règlement peut être considéré comme manquant de précision. La compréhension par les lecteurs est un élément essentiel du projet de règlement, car les informations transmises auront un impact direct sur la capacité de ceux-ci à exercer leurs droits de manière efficace en lien avec leurs renseignements personnels. Il faut cependant préciser qu'un équilibre est à atteindre entre la nécessité de détailler suffisamment les dispositions afin de permettre la rédaction de politiques de confidentialité complètes et pertinentes, et le besoin de simplicité permettant une bonne compréhension de ces dispositions. Ainsi, les ajouts qui sont proposés dans les questions suivantes devraient être considérés avec cette intention de ne pas nuire à la compréhension du projet de règlement et à son application par les organismes.	forts : (i) Il est concis. Il énonce de nouvelles normes relativement simples et il est réaliste de penser pouvoir les mettre en œuvre rapidement ; (ii) Il a une raison d'être importante ; (iii) Bon véhicule juridique, car un règlement est plus facilement amendable qu'une loi. Points faibles : (i) Dans le titre, on retrouve les termes « politique de confidentialité », mais je suis d'avis que l'on devrait plutôt parler d'un avis relatif à la protection des renseignements personnels, afin de ne pas induire le public en erreur. Je pense que le mot « avis » est sémantiquement correct, plutôt que « politique », puisque l'on parle de version qui se retrouve sur internet. Aussi, on parle des renseignements personnels, qui ne sont qu'une partie d'une sphère plus grande concernant la confidentialité. (ii) Aucune mention de ce que constitue le recueil de renseignements personnels par un moyen technologique ; (iii) Aucune mention concernant les enfants, pourtant ils utilisent les sites internet autant, sinon plus, que les adultes. Aucune règle particulière n'est applicable aux personnes vulnérables ; (iv) Aucune mention de l'importance d'utiliser un langage simple et clair et d'être transparent ; (v) Les moyens technologiques visent les témoins de connexion, mais aucune mention n'est faite dans le règlement. Il aurait pu être intéressant de préciser qu'un second avis doit être produit et rendu disponible concernant ceux-ci.
Tout d'abord, le projet de règlement présente une disposition préliminaire qui permet aux lecteurs d'avoir une bonne mise en contexte de la raison d'être des dispositions qui suivent, ce qui vient faciliter la compréhension du texte. Le projet de règlement en tant que tel respecte son champ de compétence et établit clairement le contenu des politiques de confidentialité et des avis de modification des organismes publics ainsi que les modalités entourant leur publicisation sur leur site Internet. Le projet de règlement est généralement clair quant aux exigences posées même s'il manquerait quelques définitions pour assurer une interprétation uniforme de tous. Cependant, le point négatif de ce projet de règlement est qu'aucune mention n'est faite quant à une politique de témoins de connexion (cookies) des organismes publics. Cela aurait été primordial compte tenu du fait qu'une telle politique est intrinsèquement liée à une politique de confidentialité vu leur raison d'être. De plus, le règlement s'applique aux organismes publics qui recueillent des renseignements personnels par le biais de moyens technologiques et, souvent, cette collecte est effectuée par l'entremise de témoins	La proposition d'une refonte complète soulève l'idée d'une approche commune pour l'ensemble du Canada, s'étendant idéalement à la fois au secteur public et privé. Le projet de règlement semble répondre à des besoins importants au Québec, comblant des lacunes et clarifiant des points spécifiques. Il exige que les organismes publics publient une politique de confidentialité ainsi que des avis de modification, alignant cette obligation sur les normes du RGPD, bien que le RGPD soit plus détaillé dans ses exigences. Ce projet de règlement semble refléter une approche inspirée de la common law, mettant en avant une application minutieuse de la protection des données personnelles dans le domaine de la vie privée. Cependant, vu la nature particulière de ce secteur, l'instauration d'une loi spécifique paraît nécessaire. Cette perspective d'un règlement propre n'est pas exclusive au Québec ; elle trouve également écho en Europe avec le RGPD. De telles lois sont cruciales pour équilibrer les dispositions qui pourraient potentiellement empiéter sur des droits tels que l'accès à l'information. Bien qu'il existait déjà une réglementation spécifique au Québec, une mise à

de connexion. Il serait donc nécessaire d'imposer à l'article 7 l'obligation d'apporter à l'attention de la personne concernée, le cas échéant, la politique de « cookies » de l'organisme public lors de la collecte de renseignements personnels. Cela permettrait d'éviter l'implantation d'un vide juridique pour les organismes publics ayant recours à ce moyen de collecte des renseignements personnels.	jour complète des dispositions semblait nécessaire. L'initiative de révision et d'actualisation répond à l'évolution des enjeux liés à la confidentialité et à la protection des données, garantissant une réglementation pertinente et adaptée à l'ère numérique.
De façon générale, le projet de règlement me paraît utile pour les organismes publics, car il vient préciser le contenu de la politique de confidentialité qu'ils doivent adopter et diffuser. Cependant, plusieurs améliorations pourraient y être apportées. En effet, la notion de consentement est absente du projet de règlement. Il en va de même pour les critères de nécessité et de proportionnalité. Les organismes publics doivent développer le réflexe de se questionner sur l'équilibre entre leurs intérêts légitimes à collecter des renseignements personnels et l'atteinte au droit à la vie privée des personnes concernées. De plus, l'essentiel du projet de règlement se concentre sur la confidentialité, mais néglige certains aspects du droit d'accès à l'information. D'autre part, le projet de règlement devrait porter une attention égale à l'ensemble du cycle de vie de l'information, et non seulement à la collecte des renseignements personnels. Bref, le projet de règlement atteindra sans doute partiellement son objectif ultime, soit de permettre aux citoyens d'obtenir en temps opportun les renseignements nécessaires afin de comprendre leurs droits en matière d'accès et de protection de leurs renseignements personnels. Il s'agit d'un pas dans la bonne direction.	Le projet de règlement apporte une base pour la création d'une politique de confidentialité chez les organismes publics, qui est en somme une bonne indication de la volonté de transparence de la part des organismes publics. Toutefois, il manque plusieurs informations importantes concernant, entre autres, la conservation des renseignements personnels par les organismes publics. Également, différents organismes publics ont des obligations de traitement des renseignements personnels qui peuvent différer ; par exemple, les organismes de santé et services sociaux devront souscrire également au projet de loi 3 prévoyant que les renseignements de santé ne peuvent être utilisés que par les catégories de personnes identifiées dans sa politique de gouvernance et uniquement aux fins pour lesquels ils ont été recueillis. Il ne pourrait donc pas y avoir un partage de renseignements tel qu'inscrit dans le projet de règlement. Donc, le manque d'information sur les mécanismes de collecte et de stockage des renseignements personnels fait en sorte que le projet de règlement n'est pas totalement transparent. De plus, la publicisation en ligne telle qu'inscrite dans la loi ne permettra pas à l'ensemble des utilisateurs d'y avoir accès de façon simple, à moins de mettre en place des mécanismes facilitant l'accès pour les personnes en situation d'illectronisme. Il serait donc pertinent de voir à des alternatives pour faciliter l'accessibilité. À la suite de la lecture de ce projet de règlement, il est porté à croire que les utilisateurs n'auront pas toute l'information nécessaire pour donner un consentement libre et éclairé.
Je trouve que le but du législateur de conformiser les politiques de confidentialité lorsqu'un organisme public souhaite récolter des renseignements personnels est très pertinent. Cela permet, selon moi, d'uniformiser cette pratique et d'encadrer davantage les informations devant minimalement être présentes en permettant au citoyen de mieux comprendre pour quelles raisons et dans quels contextes leurs renseignements personnels sont utilisés. Cependant, ces objectifs ne sont pas nécessairement atteints par l'entremise du	Tout d'abord, on peut remarquer que « le projet de règlement n'a pas de conséquence sur les entreprises, en particulier les PME ». Cette précision est surprenante puisque ce projet est sensé s'appliquer à la Loi sur l'accès et non à la Loi sur le secteur privé. Une confusion pourrait naître ici, notamment quant aux objectifs du législateur et à la cohérence des propos présentement critiqués. Par ailleurs, si le projet est présenté dans le cadre d'un objectif d'harmonisation, ce dernier paraît peu ambitieux. Rien n'impose que les 14 points qui doivent être

Règlement. Selon moi, les termes utilisés ne sont pas nécessairement adéquats. Prenons en exemple le terme « politique ». Habituellement, ce terme est employé pour faire référence à une politique à l'interne pour les employés. Dans un contexte où un tel texte est publié sur un site Internet (ou tout moyen technologique) pour les utilisateurs, il s'agit plutôt d'un *avis de confidentialité* visant à informer l'utilisateur des utilisations de ses données personnelles. La lecture/consultation de la « politique » ne constitue pas une obligation ou une ligne directrice à respecter, mais bien seulement un avis à titre **informatif**. Pour d'autres raisons qui seront abordées dans les sections subséquentes, je crois que ce projet de règlement contient un grand manque de cohérence et de clarté par rapport aux autres lois.	respectés le soient dans un ordre et un format prédéterminé. Ceci aurait pourtant facilité la compréhension, et donc, renforcé le consentement des citoyens face aux politiques de confidentialité. Ensuite, concernant les modifications, on semble inclure toutes les modifications, même celles qui n'ont pas d'impact sur le consentement, comme une coquille dans le texte (sans modification du sens) ou d'autres modifications comme la police, la mise en page, etc. Enfin, on n'est pas vraiment harmonisé avec la Loi sur le secteur privé. Rien ne vient clarifier la question du consentement des mineurs. De plus, le législateur qui a permis ce règlement pour le secteur public et pas pour le secteur privé, pose question quant à la collaboration entre les deux secteurs, notamment en ce qui concerne les transferts de données en santé lorsque des patients passent du secteur public au secteur privé. Un nouveau consentement devrait être recueilli à chaque fois qu'un transfert a lieu.
À titre d'évaluation générale, le projet de règlement favorise l'uniformisation du contenu et des modalités des politiques de confidentialité des organisations publics, tel que prévue à l'article 15 de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (« *Loi 25* ») modifiant l'article 63.4, alinéa 2, de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (« *Loi sur l'accès* »). De plus, ce projet de règlement répond aux nouvelles exigences législatives instaurées par la *Loi 25* à la *Loi sur l'accès*. Le contenu minimal exigé témoigne de la qualité attendue des politiques de confidentialité des organisations publics faisant preuve de l'importance accordée au consentement éclairé et à la sécurité des données personnels dans un contexte numérique. De plus, l'usage de neutralité technologique au sein de ce projet de règlement assure une pérennité de son application à travers le temps, en égard à l'évolution rapide et constante technologique, qui a autrefois entrainé certains enjeux législatifs. Toutefois, il m'est impossible d'accorder une note plus élevée à ce projet de règlement, en considérant que certains éléments, qui seront abordés et élaborés dans les questions suivantes, incluant le champ d'application, la collecte commune de renseignements personnels ou encore les avis de modifications pourraient entrainer des problèmes en lien avec la mise en application de l'entièreté de ce projet de règlement, dans sa version actuelle.	Plusieurs organismes ont fait part de leur intérêt à obtenir un règlement qui précise davantage la portée de l'article 63.4 *Loi sur l'accès* (Barreau, FQM). Ce règlement répond à une préoccupation qui est bien réelle. En effet, selon le Commissariat à la protection de la vie privée, une politique de confidentialité met en œuvre le principe de transparence au profit des citoyens. Pour se faire, la politique se doit d'être exhaustive (Cpvp). En revanche, le règlement oublie plusieurs enjeux importants qui nécessitent une clarification. En effet, celui-ci apporte très peu de précisions en lien avec l'exigence d'une rédaction simple et claire. Dans ce sens, afin d'accroître la transparence avec les citoyens, il aurait été souhaitable de clarifier cette exigence, notamment en prescrivant une approche par couche, ou par sections (ex. : droits des usagers). Le citoyen souhaitant s'informer davantage pourrait ainsi accéder facilement au contenu recherché. Plus encore, l'article 2 contient certaines lacunes au niveau du contenu minimal d'une politique (voir 2.2). Dans un esprit d'harmonisation, il aurait été souhaitable de prévoir une forme particulière pour mieux guider les organismes. À cet égard, une annexe au règlement ou une ligne directrice aurait bien répondu au besoin. Pour illustrer ces propos, il convient de faire une analogie avec l'étiquette alimentaire. Sans chercher ce niveau de détail, une certaine forme d'harmonisation aurait permis au « consommateur moyen plutôt pressé » de prendre connaissance des faits saillants d'une politique de confidentialité et chercher plus d'informations au besoin.

1.2 Le projet de règlement vous parait-il valide du point de vue juridique ? Les orientations qu'il donne sont-elles cohérentes entre elles ?

D'un point de vue juridique, le seul article de la Loi sur l'accès (art. 63.4) concernant les politiques de confidentialité mentionne qu'une telle politique doit être « rédigée en termes simples et clairs » et qu'un règlement du gouvernement peut en déterminer le contenu et les modalités. Le projet de règlement me parait donc valide en ce sens, car ce dernier vient effectivement déterminer le contenu et les modalités et les termes utilisés sont pour l'ensemble simples et clairs. Toutefois, certaines dispositions du projet de règlement semblent aller au-delà de la Loi sur l'accès. En effet, la loi (art. 65) mentionne que lors de la collecte de renseignements personnels auprès de la personne concernée, celle-ci doit être informée de certains éléments précis, tandis que d'autres éléments doivent plutôt lui être transmis si elle en fait la demande. Selon le projet de règlement, le contenu d'une politique de confidentialité inclut des éléments faisant partie de ces deux catégories. Il semble donc y avoir ici une certaine incohérence, l'organisme devant fournir en tout temps dans sa politique de confidentialité des informations selon le projet de règlement (ex : catégories de personnes qui ont accès aux renseignements), mais seulement les transmettre sur demande selon la loi. Considérant que la politique de confidentialité doit être portée à l'attention de la personne concernée lors de la collecte (art. 7 projet de règlement), ces informations ne sont donc plus transmises sur demande.	Après une évaluation générale du projet de règlement, je considère que ce dernier est valide du point de vue juridique et, outre une petite incohérence avec la Loi sur l'accès (voir 2.3.), il est en conformité avec la loi applicable en l'espèce. Ce règlement découle directement de l'article 63.4 de la Loi sur l'accès qui prévoit que la politique de confidentialité doit être rédigée en termes simples et clairs. Dans les faits, le législateur a réussi sur ce point puisqu'il a conçu un règlement concis et bien détaillé, bien que ce dernier nécessite certaines précisions et ajouts. Pour ce qui est de l'incohérence avec la Loi sur l'accès, elle concerne la disposition sur la collecte commune des renseignements personnels. Entre autres, elle impose des obligations de consentement et de responsabilité, mais ne donne pas de précision sur les modalités de gestion en cas de collecte commune. Concernant les orientations du projet de loi, je suis d'avis que les dispositions sont tout de même toutes cohérentes entre elles. Par exemple, une attention particulière est accordée à la publicisation et à la consultation (par le CAI) des politiques de confidentialité ainsi que des avis de modification, ce qui renforce le principe de transparence et la protection des renseignements personnels.
Le projet de règlement me paraît valide du point de vue juridique. En effet, il est édicté en conformité avec l'article 63.4 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après « LAI ») qui indique qu'« [u]n règlement du gouvernement peut déterminer le contenu et les modalités de cette politique [de confidentialité] et de cet avis [de modification] ». Le projet de règlement vient effectivement édicter le contenu et les modalités de la politique et de l'avis. Toutefois, il semble y avoir une petite ambiguïté dans le projet de règlement. En effet, l'article 63.4 LAI intègre le principe de neutralité technologique, avec les termes « par tous moyens propres à atteindre les personnes concernées », alors que dans le projet de règlement, on ne fait référence qu'à la publicisation de la politique et de l'avis sur le site Internet. Il serait plus	L'article 64.3 de la *Loi sur l'accès* autorise le gouvernement à adopter un règlement qui précise les modalités et le contenu de la politique de confidentialité et de l'avis de modification. Sur ce point, le projet de règlement est conforme à sa loi habilitante. De plus, les orientations énoncées dans ce projet de règlement sont généralement cohérentes entre elles. Néanmoins, certaines incohérences subsistent. Notamment, le fait que les organismes effectuant une collecte commune ou recueillant des renseignements pour d'autres puissent élaborer une politique de confidentialité commune n'est pas clairement reflété dans le contenu exigé dans celle-ci. Par exemple, l'article 2 ne prévoit pas l'obligation d'indiquer qu'il s'agit d'une collecte commune de renseignements personnels. Aussi, le projet de règlement ne semble pas prendre en compte l'éventualité où les modalités de la collecte

cohérent que le règlement intègre le même vocabulaire que la disposition habilitante. Autrement, le projet de règlement paraît valide d'un point de vue juridique, car il respecte l'esprit et le but de la loi habilitante. De plus, tel qu'énoncé dans son préambule, le projet de règlement permet au citoyen d'avoir, par la politique, des informations sur le traitement de ses renseignements personnels, pour assurer le bien-être commun. Finalement, l'application du projet de règlement semble également réaliste pour les organismes publics visés.	diffèrent entre les organismes qui font une collecte commune. De plus, le projet de règlement prévoit qu'on doit consulter le comité instauré à l'article 8.1 de la *Loi sur l'accès* avant de publier une politique de confidentialité ou un avis de modification significative sur son site internet. Or, dans les faits, ces documents vont vraisemblablement être rédigés par le comité lui-même, en particulier dans le cas de petites organisations. Cette situation crée donc une certaine incohérence à l'article 5 du projet de règlement. De plus, bien que l'alinéa 3 de l'article 8.1 de la *Loi sur l'accès* prévoit que certains organismes peuvent être exclus de l'obligation de former un comité, on ne prévoit pas cette éventualité dans ce règlement.
D'abord, ce règlement peut bel et bien être édicté en vertu du nouvel article 63.4 de la Loi sur l'accès (introduit par la Loi 25), qui précise qu'« un règlement du gouvernement peut déterminer le contenu et les modalités de cette politique et de cet avis. » Ensuite, je suis d'avis que les orientations du projet de règlement sont cohérentes entre elles : elles militent toutes vers des politiques de confidentialité mieux encadrées. Néanmoins, elles ne sont pas parfaitement alignées sur les objectifs plus grands que vise le règlement, soit d'améliorer l'accès aux renseignements personnels pour les utilisateurs et de procéder à une harmonisation générale des politiques de confidentialité québécoises. Ce règlement est également cohérent avec l'esprit de la Loi 25, soit avec l'idée d'être plus stricts à l'égard de la protection des renseignements personnels. Il est vrai que des écarts avec la loi canadienne sont créés et que la législation québécoise se rapproche alors davantage du courant européen (RGPD), notamment en lien avec les critères de validités du consentement qui jouent un rôle important dans les politiques de confidentialité (ex. article 14 de la Loi sur le privé et article 4.3.6 Annexe 1, LPRPDE). Toutefois, cela n'affecte pas la cohérence ou la validité juridique du projet de règlement pour autant, d'après moi.	Selon moi, le projet de Règlement comporte des incohérences. Le point focal de cette note est tout ce qui a trait aux témoins de connexion, soit les « cookies ». On ne retrouve aucune mention faite à leur égard dans le Règlement, pourtant, selon moi, il est primordial d'ajouter une section sur les cookies dans toute politique de confidentialité qui pourra référer en hyperlien à une annexe qui explique les différents témoins de connexion sous forme de tableau. D'abord, en allant voir dans la *Loi sur le secteur privé*, il est possible de comprendre que selon l'art. 9.1, les témoins de connexions ne nécessitent pas de paramètres de confidentialité par défaut alors que l'art. 8.1 précise que tout renseignement personnel (**profilage**) devrait être désactivé par défaut. Il y a ici une incohérence puisque les témoins de connexion constituent, dans certains cas, des données permettant le profilage d'une personne pour faire de la publicité ciblée. C'est la raison pour laquelle, malgré les articles présents dans la *Loi sur le secteur privé*, que les témoins de connexion devraient être inclus dans le projet de Règlement. Il me semble pertinent de mentionner à l'utilisateur la portée de l'utilisation de ses renseignements personnels par rapport aux cookies afin d'obtenir un consentement bel et bien valide. Avec l'ajout d'une telle mention, le Règlement serait selon moi plus complet et cohérent du point de vue juridique.
L'article 92 de la *Loi constitutionnelle de 1867* donne aux provinces les pouvoirs de légiférer pour la santé, les institutions municipales, les matières de nature purement locale, entre autres. Ainsi, le Québec avait la possibilité de légiférer dans le secteur public de la province, et donc la *Loi sur l'accès aux documents publics et sur la protection des renseignements personnels* seraient une loi valide, et les règlements qui en découlent le serait aussi. Le projet de règlement	Je suis d'avis qu'il manque de cohérence entre la Loi sur l'accès et le projet de règlement. À titre d'exemple, en vertu de l'article 65 de la Loi sur l'accès, la personne concernée est informée des catégories de personnes qui ont accès aux renseignements personnels au sein de l'organisme public et des coordonnées du responsable de la protection des renseignements personnels sur demande alors que l'article 2 du projet de règlement indique que les informations

s'applique dans le secteur public québécois, tel que prévu dans la loi habilitante, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (ci-après *Loi sur l'accès)* à l'article 1 et 1.1. L'article 155 al. 1(6) donne le pouvoir au gouvernement du Québec d'établir un règlement concernant les politiques de confidentialité. Ainsi, le projet de règlement vient préciser certains aspects aux politiques de confidentialité qui proviennent de cet article. Le règlement est cohérent avec les orientations des politiques de confidentialité dans le secteur public déjà demandées par la loi habilitante, et viennent simplement ajouter des obligations concernant ceux-ci. L'article 63.4 de la *Loi sur l'accès,* qui sera en vigueur à partir du 22 septembre 2023, demande que les organismes publics qui recueillent des renseignements personnels, publient une politique de confidentialité. Le règlement vient donc préciser ce que ces politiques devraient contenir, comment elles devraient être publiées, et comment les modifications doivent se faire.	mentionnées ci-dessus doivent être incluses dans la politique de confidentialité de l'organisme public. Je réfère à une autre incohérence entre la Loi sur l'accès et le projet de règlement dans ma réponse à la question 2.5. Je suis également d'avis que l'article 1 du projet de règlement comporte une invalidité sur le plan juridique. L'article 1 mentionne que pour l'application du projet de règlement, l'expression « organisme public » comprend un ordre professionnel. Je suis d'avis qu'un ordre professionnel n'est pas un organisme public. On aurait très bien pu préciser que le projet de règlement s'applique aux ordres professionnels dans la mesure prévue par le Code des professions sans pour autant mentionner que ce sont des organismes publics. Cette façon de faire serait également plus cohérente avec la Loi sur l'accès. Bien que la Loi sur l'accès s'applique aux ordres professionnels, dans la mesure prévue par le Code des professions, la Loi sur l'accès n'inclut pas un ordre professionnel dans sa définition d'organisme public.
La Loi sur l'accès, à son article 63.4, permet au gouvernement de prendre un règlement pour déterminer le contenu et les modalités d'une telle politique (et/ou de son avis de modification). Un règlement n'a pas d'autonomie propre et il doit respecter la loi habilitante qui l'autorise à agir. En l'espèce, on se trouve face à une habilitation spéciale (et non générale) qui vise un objet, soit celui de régir la forme et les modalités que la politique aura. C'est ce que le règlement fait. Par contre, il existe certaines incohérences entre le texte de la loi habilitante et le projet de règlement. D'abord, l'article 63.4 prévoit que l'organisme public « doit publier sur son site Internet et diffuser par tout moyen propre à atteindre les personnes concernées ». Le projet de règlement parle seulement de publier la politique sur le site internet de l'organisme (article 6). De plus amples commentaires seront faits plus tard, mais il me semble que ce ne soit pas suffisant comme moyen pour atteindre toutes les personnes concernées. L'article 63.4 fait également mention de l'importance de rédiger la politique en termes clairs et simples. Aucune mention de cet aspect n'est faite dans le règlement. Il transparaît au contraire du texte du règlement que les politiques seront longues, puisque l'article 2 à lui seul prévoit 14 éléments qui devront obligatoirement figurer dans la politique.	Le projet de règlement est valide en ce qui concerne les conditions de forme et de fond puisqu'il y a un fondement juridique qui autorise sa mise en place, soit l'article 63.4 de la Loi sur l'accès, et que ses dispositions visent à atteindre les objectifs qui lui sont attribués qui constituent de déterminer le contenu et les modalités des politiques de confidentialité et des avis de modification des organismes publics. Bien que le projet de règlement attribue plusieurs obligations aux organismes publics, il subsiste toutefois une incohérence quant au caractère contraignant de ces dispositions. En effet, aucune mesure de contrôle n'est prévue dans le projet de règlement pour vérifier le respect du contenu et des modalités entourant les politiques de confidentialité et les avis de modification. Même si les articles 162 et 158 de la *Loi sur l'accès* prévoient des sanctions pour la contravention des règlements pris en conformité avec la Loi, aucune conséquence n'est réellement possible sans dispositif de contrôle officiel. Ainsi, le projet de règlement n'est pas assez contraignant pour les organismes publics dont la surveillance de leurs pratiques retomberait seulement sur le bon-vouloir des individus qui se rendraient compte du caractère illégal des documents qui sont mis à leur disposition et qui prendraient la peine d'effectuer une plainte selon le processus établi par l'organisme en vertu de l'article 63.3 de la *Loi sur l'accès*.
Le projet de règlement me semble conforme à la loi et donc valide du point de vue juridique. De	À première vue, le règlement semble valide puisque sa loi habilitante (*Loi sur l'accès*) prévoit

plus, les orientations semblent cohérentes. L'analyse de la validité juridique a été effectué en considérant les modifications législatives apportées par la *Loi 25*, qui entreront officiellement en vigueur le 22 septembre 2023, et ainsi représentera le cadre légal lors de l'entrée en vigueur du présent projet de règlement. Le projet de règlement permet de « déterminer le contenu et les modalités » d'une politique de confidentialité et d'un avis de modification par réglementation, tel que prévu à l'article 15 de la *Loi 25* modifiant l'article 63.4, alinéa 2, de la *Loi sur l'accès* et à l'article 155, alinéa 1, paragraphe 6, de la *Loi sur l'accès*. De plus, la politique de confidentialité fournit des informations essentielles à l'obtention du consentement éclairé à la collecte de renseignements personnels par un moyen technologique, tel qu'obligatoire, en vertu de l'article 53, alinéa 1 de la *Loi sur l'accès*, et ainsi l'information transmise par les organismes à travers ces politiques sont encadrés par cette même loi. En effet, le contenu, ou l'information minimal requis dans la politique par le projet de règlement est conforme aux exigences prévues, en vertu de l'article 18, de la *Loi 25*, qui engendrera des modifications à l'article 65 de la *Loi sur l'accès*.	la possibilité de préciser davantage la portée de l'article 63.4. En revanche, à la lecture des articles de la *Loi sur l'accès*, il est possible de constater plusieurs références à un éventuel règlement du gouvernement (article 63,2, 63,3, 63,4, 63,8). Par soucis de simplicité et d'exhaustivité, il aurait été souhaitable de rassembler ces prescriptions règlementaires au même endroit. Dans ce sens, peut-être aurait-il été préférable de procéder par l'entremise de lignes directrices. Comme c'est la CAI qui est chargé de surveiller l'application de la loi (art. 122.1), celle-ci est certainement bien placée pour déterminer l'étendue des obligations découlant des articles précités. Autrement dit, il aurait été souhaitable de lui laisser établir des lignes directrices selon ses propres orientations, compte tenu de son expertise dans la matière. Pour pousser la réflexion davantage, une approche plus cohérente avec l'objectif d'harmonisation nécessiterait une meilleure conformité avec les principes proposés par le RGPD. En effet, ce dernier met en œuvre des standards reconnus à l'international. À cet égard, le projet de règlement échoue à mettre de l'avant certains principes (consacrés par l'article 5 RGPD), comme celui de la responsabilité, loyauté, minimisation des données et de la transparence. En tenant compte de ces principes, le règlement apporterait une meilleure cohérence des politiques de confidentialité avec les exigences internationales, au profit du citoyen qui bénéficierait d'une présentation de ses droits réellement harmonisée.
J'évalue assez sévèrement cet aspect spécifique du projet de règlement, car la cohérence entre le projet de règlement et la *Loi sur l'accès* est parfois faible. À titre d'exemple, l'article 6 du projet de règlement mentionne clairement l'obligation de publier la politique de confidentialité, ainsi que tout avis de modification, dans une section dédiée du site Internet de l'organisme. Ceci s'inscrit en cohérence avec l'article 63.4 de la *Loi sur l'accès.* Cependant, 63,4 mentionne non seulement l'obligation des organismes de publier ces informations sur leur site Internet, mais également de la diffuser par tout moyen propre à atteindre les personnes concernées. Aucune disposition du projet de règlement ne s'attarde à cette obligation. Bien que l'article 7 du projet de règlement mentionne de surcroît que la politique, ainsi que tout avis de modification de celle-ci, doivent être portés à l'attention de la personne au moment de la collecte de renseignements personnels, cela semble insuffisant pour répondre aux exigences de la *Loi sur l'accès*. Le projet de règlement devrait également exiger des	Le projet de règlement semble s'inscrire dans un cadre juridique approprié en respectant les lois auxquelles il fait référence. Cependant, il est important de noter que l'objectif d'un règlement est souvent spécifique et peut avoir des implications importantes dans sa mise en œuvre. Un point de divergence notable est l'absence de distinction claire entre les renseignements personnels et les cookies. Cette absence de distinction peut susciter des interrogations quant à la manière dont ces deux types de données sont traités et protégés. En comparaison, le RGPD offre une distinction nette entre les données personnelles et les cookies, apportant ainsi une cohérence et une clarté accrues. Une autre préoccupation concerne l'absence de distinction entre l'accès aux documents et les renseignements personnels. Cette absence de distinction peut entraîner des conflits potentiels dans la gestion des données et l'accès aux informations. Une séparation claire entre ces deux catégories de données peut contribuer à éviter les confusions et à garantir un traitement approprié des données. En résumé, bien que le

organismes que leur politique de confidentialité contienne une référence à leurs propres obligations en cas d'incident de confidentialité, conformément à l'obligation prévue à l'article 63.8 de la *Loi sur l'accès*. La politique devrait également énoncer les obligations et engagements de l'organisme envers leurs employés en matière de formation et de soutien à l'application de la politique, tel que stipulé à l'article 63.3 de la *Loi sur l'accès*.	projet de règlement respecte les normes juridiques en vigueur, il est essentiel de reconnaître que son objectif particulier peut entraîner des questions significatives. L'absence de distinction entre les renseignements personnels et les cookies, ainsi que l'absence de séparation entre l'accès aux documents et les données personnelles, peuvent soulever des préoccupations quant à la clarté et à la cohérence du règlement.
Le projet de loi respecte les grandes lignes de la mise en place de politiques de confidentialité telles que décrites dans la loi privée québécoise et le RGPD. Toutefois, plusieurs orientations ne sont pas cohérentes en lien avec l'objectif de la protection de la vie privée et la notion de transparence. D'abord, la mention de collecte commune ne respecte pas l'art 4.3.4 de la LPRPDE mentionnant qu'une entreprise doit mettre en place des mesures de sécurité selon le degré de sensibilité des renseignements personnels et doit élaborer des modes de sécurité par des moyens physiques, administratifs, ou techniques. Or, le degré de sensibilité des renseignements personnels obtenus par l'ensemble des organismes publics n'est pas similaire. Par exemple, les services de santé ont accès à des données biométriques dont les ordres professionnels n'ont pas accès. De plus, les utilisateurs consentent à la collecte de leurs renseignements seulement dans un but précis. De plus, le projet de loi 3 prévoit qu'un organisme de santé doit faire une évaluation des facteurs relatifs à la vie privée lorsque le contrat de service implique une communication de renseignements de santé à l'extérieur du Québec ce qui n'est pas mentionné dans le présent projet de règlement. Il est donc primordial que la politique de confidentialité des services de santé se doit d'avoir cette mention. En connaissance de l'ensemble des lois applicables aux services publics, il est impossible de croire que la collecte commune serait juridiquement faisable.	Ce projet ne parait pas valide d'un point de vue juridique. En relation avec notre critique précédente sur la présence du terme de PME dans ce projet, il nous semble que les rédacteurs sous-entendent que le les entreprises du secteur privé, à l'exclusion des PME, pourraient être impactées par le projet de règlement. Aussi, on note que dans la Loi sur le secteur privé, aucune possibilité de règlementation n'est prévue concernant les politiques de confidentialité. On pourrait se demander si le législateur insinue que les grandes entreprises privées devraient être impactée par le règlement destiné au secteur public, ce qui ne fait juridiquement aucun sens. Si l'heure est à l'harmonisation, comme le démontre le RGPD pour qui l'ensemble des règles s'appliquent aussi bien au secteur public qu'au secteur privé, on penserait que le projet de règlement essaye de rattraper des choix législatifs antérieurs. Par ailleurs, des enjeux se posent en termes de consentement : (i) Le règlement ne distinguant pas les fins essentielles des fins non essentielles, il ne permet pas de paramétrage par défaut. (ii) On n'exige pas que les utilisateurs consentent expressément aux modifications de la politique de confidentialité. Or, le consentement ne devrait pas être tacite ici. (iii) Aucun critère ne vient encadrer le motif, de réduction du délai de 15 jours pour modifier une politique de confidentialité, alors n'importe quel motif semble valable. La LCCJTI s'appliquant, il aurait été opportun d'énoncer une disposition sur les précautions particulières prises pour les données biométriques.

1.3 Le projet de règlement a-t-il une portée adéquate compte tenu de son objectif ? Est-il complet ?

L'objectif visé du projet est de déterminer le contenu et les modalités de la politique de confidentialité. Pour ce qui est de déterminer le contenu, le projet est plutôt clair sur ce qui est attendu. L'énumération des éléments que doit minimalement contenir une politique de renseignement permet une harmonisation des politiques de confidentialité des organismes	L'article 63.4 de la LAI édicte l'objet du projet de règlement est de préciser le contenu et les modalités de la politique de confidentialité et de l'avis de modification. Dans le mémoire au conseil des ministres (juin 2023, lien), il y est indiqué que l'objectif principal poursuivi par le projet de règlement est de favoriser la transparence des organismes publics lors d'une collecte de

publics et une vérification simple de la complétude de ces politiques lors de leurs élaborations est favorisée. On peut cependant regretter qu'une structure de base avec un ordre préétablit obligatoire des éléments à retrouver ne soit pas proposée. Un descriptif de ce qui doit apparaître en langage simple et clair pourrait être complété par : des définitions de termes, l'utilisation d'hyperliens et tableaux venant compléter la politique. Tout ceci permettrait une meilleure harmonisation des politiques de confidentialité au sein des organismes publics tout en garantissant une meilleure compréhension du public, ce qui renforcerait le consentement des individus concernés. Cependant, il semble que la liste des éléments minimaux que doit contenir une politique de confidentialité est incomplète. Il manque : (i) « Prévoir les rôles et les responsabilités des membres de son personnel tout au long du cycle de vie de ces renseignements ». (ii) « Une description des activités de formation et de sensibilisation que l'organisme offre à son personnel ». (iii) Les mesures de protection à prendre à l'égard des renseignements personnels lors de sondages. (iv) Des dispositions particulières relatives aux données biométriques.	renseignements personnels par des moyens technologiques. D'ailleurs, la CAI rappelle l'importance du principe de transparence en lien avec la protection des renseignements personnels, particulièrement pour les organismes publics, comme les autorités gouvernementales, en raison des pouvoirs qui leur sont accordés (2020, lien). Ensuite, dans le mémoire précédemment cité, il est indiqué que le projet de règlement permet d'harmoniser le contenu auquel les citoyens ont accès lors de la collecte de leurs renseignements personnels. Tous ces objectifs sont d'ailleurs mentionnés dans le préambule de projet. Ainsi, le projet de règlement a une portée adéquate en ce sens, car il prévoit un contenu minimal à intégrer dans les politiques de confidentialité des organismes publics. Toutefois, la CAI a dernièrement rappelé l'importance cruciale, surtout dans l'ère numérique, d'une protection renforcée des renseignements personnels des personnes mineures. Elle en fait notamment mention dans un rapport analysant la suffisance de cette protection dans la LP (août 2022, lien). Il aurait été pertinent que le projet de règlement adresse également cet enjeu, pour le secteur public, en incluant, par exemple, une notion de public cible.
À mon avis, le projet de règlement a atteint son objectif premier, qui était de préciser le contenu minimal requis dans la politique de confidentialité d'un organisme public qui collecte des données personnelles par un moyen technologique. Cependant, dans son mémoire, Monsieur Jean-François Roberge (2023) souligne que le projet de loi vise également à informer les utilisateurs de leurs droits et de la manière dont leurs renseignements personnels sont traités. Je crois que cet objectif est moins bien réalisé. Notamment, l'article 8,1 *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après « *Loi sur le secteur privé* ») prévoit qu'une entreprise qui recueille des renseignements personnels doit déclarer si elle utilise une technologie qui localise, identifie ou permet d'effectuer du profilage. Selon moi, le règlement aurait dû prévoir une disposition destinée au secteur public qui précise que les politiques de confidentialité doivent contenir ces renseignements. De plus, le projet de règlement ne traite pas du consentement pour les enfants de moins de 14 ans. Or, à mon avis, il s'agit d'un élément important pour permettre aux individus de comprendre leur droit. Ainsi, Il aurait été pertinent de prévoir une mention spécifique dans la politique de confidentialité pour ces usagers. Un autre aspect qui aurait été pertinent à aborder est une mention dans la politique de confidentialité qui prévoit que l'usager ait le droit	Selon moi, la portée du projet de règlement n'est pas tout à fait adéquate au regard de ses objectifs. Ce règlement vise à préciser le contenu des politiques de confidentialité des organismes publics, à harmoniser celles-ci entre organismes et à augmenter la transparence dont ces derniers font preuve. Il a été précisé que cela n'avait aucun impact sur les entreprises, en particulier les PME. On pourrait insinuer que le gouvernement ne souhaitait pas ajouter un fardeau administratif sur les épaules de ces dernières, mais il n'est pas très clair pourquoi (la survie des PME est-elle plus importante que la protection des renseignements personnels des citoyens ?). Cette partie est assez floue. Pour ces objectifs poursuivis, la portée s'avère plutôt adéquate, puisqu'on ne souhaitait viser que les organismes publics. Toutefois, j'aimerais apporter à votre attention les objectifs « plus larges » de ce projet. J'ai effectivement remarqué des objectifs plus étendus en consultant le préambule. « Ces politiques [aux utilisateurs] permettent également d'obtenir les informations nécessaires afin qu'ils puissent comprendre leurs droits et de quelle façon leurs renseignements personnels sont recueillis et utilisés ». Le mémoire de Jean-François Roberge énonce que tout le monde devrait avoir accès aux mêmes informations lors d'une collecte (Mémoire au Conseil des ministres). Dans cette optique, ne

à une mesure d'accommodement raisonnable pour avoir accès à ces renseignements personnels comme le prévoit notamment l'article 10 de la *Loi sur l'accès*.	serait-il pas profitable d'étendre ce règlement au secteur privé pour que tous les utilisateurs puissent profiter de ces mêmes avantages ? En somme, le projet n'est pas complet puisque, entre autres, il devrait étendre son champ d'application.
Comme mentionné dans les débats parlementaires, l'objectif du projet de loi 64 (Loi 25) est notamment de moderniser les deux principales lois (Loi sur l'accès et Loi sur le secteur privé) qui encadrent la protection des renseignements personnels des Québécois afin que celles-ci protègent mieux les Québécois à la lumière des avancées technologiques que nous avons vécues depuis l'adoption de ces deux lois. Ainsi, je suis d'avis que le législateur n'a pas suffisamment tenu compte des avancées technologiques dans son projet de règlement en s'abstenant d'élaborer des exigences particulières lorsqu'un organisme public recueille des renseignements personnels en ayant recours à une technologie comprenant des fonctions permettant d'identifier, de localiser ou d'effectuer le profilage d'une personne. En vertu de l'article 65.0.1. de la Loi sur l'accès, un organisme public qui a recours à une telle technologie doit au préalable informer la personne concernée du recours à une telle technologie et des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage. Je suis d'avis que le projet de règlement aurait également dû encadrer le recours à la biométrie. L'article 44 de la LCCJTI prévoit l'obligation d'obtenir le consentement exprès de la personne concernée avant de recourir à la biométrie pour vérifier ou confirmer l'identité de la personne concernée.	L'objectif du Projet de Règlement est d'harmoniser les pratiques afin que les utilisateurs puissent rapidement se retrouver et avoir des balises objectives afin de guider leur comportement. Je ne comprends pas pourquoi sa portée est limitée aux organismes publics. Les utilisateurs auront tout aussi souvent des interactions avec le secteur privé qui les mener à donner leur consentement à la récolte de leurs renseignements personnels via des moyens technologiques. Je pense qu'il devient rapidement difficile pour l'utilisateur moyen de se retrouver à travers des politiques. Afin de de diminuer les comportements en lien avec la lassitude du consentement, il serait opportun d'offrir un modèle type pour tous qui serait prescrit par règlement. Je pense également que le règlement possède des lacunes au niveau de son contenu. Par exemple, il aurait été intéressant de retrouver dans le règlement des règles de forme afin de s'assurer que toutes les politiques présentent les mêmes caractéristiques et que les utilisateurs puissent facilement s'y retrouver. On passe également carrément à côté des témoins de connexion. Pourtant, les organismes publics en font assurément usage. Il serait intéressant que les organismes publics soient également tenus de référer à leur politique en matière de témoins de connexion lorsque l'on utilise leur site internet. À mon avis, cet avis devrait être présenté dans un document à part de la politique de confidentialité, pour éviter toute confusion pour l'utilisateur.
Le projet de règlement « vise à déterminer le contenu et les modalités » d'une politique de confidentialité et d'un avis de modification. De plus, pour les citoyens, le règlement doit permettre « d'harmoniser le contenu des politiques », « d'obtenir les informations nécessaires afin [de] comprendre leurs droits » et de comprendre « de quelle façon leurs renseignements personnels sont recueillis et utilisés ». Le projet de règlement semble donc adéquat, permettant l'atteinte de cet objectif et de ces visées. Toutefois, une section additionnelle pourrait être ajoutée. Afin d'assurer l'accessibilité, il serait pertinent d'ajouter une section quant à la visibilité et la facilité de trouver une politique sur un site Internet. Aucune mention n'est faite à ce sujet, il est seulement indiqué qu'une telle politique doit être publiée	L'objectif du règlement est « d'harmoniser le contenu des politiques de confidentialité des organismes publics ». Ainsi, la portée du projet de règlement devrait demander aux organismes publics de publier une politique de confidentialité claire et précise, permettant ainsi aux citoyens dont les données seront recueillies de connaitre leurs droits et de savoir comment leurs renseignements personnels seront utilisés. Le règlement s'applique aux organismes publics ainsi qu'aux ordres professionnels, tel que prévu à son article 1, faisant ainsi référence aux articles 1 à 7 de la *Loi sur l'accès.* L'article 3 de cette loi exclut des organismes publics les tribunaux. Le règlement est particulièrement précis, et s'applique seulement aux politiques de confidentialité pour les organismes publics qui recueillent des renseignements personnels par un

dans une section qui lui est dédiée (art. 6 projet de règlement). Une mention pourrait également être ajoutée précisant qu'un lien menant à la politique devrait se retrouver non pas seulement sur la page d'accueil du site Internet, mais également en bas de chaque page du site, permettant ainsi son accès à tout moment durant la navigation. La LPRPDE (art. 4.8 et 4.8.1, annexe 1) mentionne justement qu'une « personne doit pouvoir obtenir sans efforts déraisonnables de l'information au sujet des politiques ». De plus, le Commissariat à la protection de la vie privée du Canada recommande de placer « à un endroit en évidence » le lien donnant accès à la politique de confidentialité.	moyen technologique. Puisqu'il s'agit d'un règlement qui assurera que le public soit protégé en ayant accès à une politique de confidentialité public, celui-ci aurait pu être écrit de manière plus large. Par exemple, ce règlement exclut tous les renseignements qui sont récoltés par des moyens autre que technologiques, tel que par remplissage de documents « papiers ». Ces documents peuvent eux-aussi contenir des renseignements personnels, mais ne seront pas inclus dans le projet de règlement. Je considère aussi que certains éléments sont manquants. Par exemple, le projet de règlement ne mentionne aucunement l'anonymisation et la destruction des renseignements personnels. Cela serait pertinent à ajouter dans le projet de règlement pour que les politiques de confidentialité les prennent en compte, afin d'assurer l'harmonisation des durées de conservation.
Le projet de règlement a une portée adéquate car l'objectif est de réglementer les politiques de confidentialité des organismes publics et donc de permettre une plus grande transparence sur les renseignements personnels que ces organismes collectent auprès de leurs utilisateurs. Toutefois, il n'est pas complet si on compare avec d'autres juridictions qui ont déjà fait cette analyse, par exemple l'Union européenne, par le RGPD, qui ajoute des points importants quant au traitement des renseignements personnels. Par exemple, sur l'aspect du droit à l'oubli qui permet aux utilisateurs de retirer leur consentement en lien avec la collecte de leurs renseignements. De telle disposition ne sont pas notées dans le projet de règlement, bien que le droit à la désindexation (oubli) soit prévu à la version privée de la Loi 25 du secteur privé. Il est possible pour les utilisateurs de demander à ce que leurs renseignements soient retirés de la banque d'information, à certaines conditions. Présentement, dans le projet de règlement, il y a seulement une notion de rectification et d'accès aux données. Aucun mécanisme ne permet de retirer le consentement. Cette possibilité de désindexation devrait être indiquée à la politique de confidentialité car elle permet aux utilisateurs de connaître leurs droits concernant le consentement qu'ils ont donné, et donc de s'assurer de la notion de consentement éclairé. En somme, le projet a une portée adéquate, mais n'est pas complet.	Dans le préambule du projet de règlement, il est mentionné que le règlement permet d'harmoniser le contenu des politiques de confidentialité des organismes publics. En plus de l'harmonisation des politiques, le projet avait également pour objectif de donner aux citoyens les informations nécessaires pour qu'ils puissent comprendre leurs droits. Dans son ensemble, je suis d'avis que le règlement couvre bien tous les éléments nécessaires pour accomplir son objectif. Cependant, afin de mieux remplir l'objectif d'harmonisation, je pense que le secteur privé devrait être inclus en partie. En effet, si le secteur public est assujetti aux mêmes exigences en ce qui concerne le contenu des politiques de confidentialité, les personnes concernées pourraient profiter de politiques claires et similaires entre elles, ce qui en faciliterait la consultation. De plus, afin de mieux accomplir l'objectif du règlement qu'est de donner aux citoyens le plus d'informations possible sur leurs droits, il existe une belle opportunité avec ce règlement de mettre en place un encadrement autour des témoins de connexion puisqu'il n'existe aucune législation portant sur ce sujet au Québec. Bien que les lois applicables en matière de protection des renseignements personnels n'exigent pas que les organismes publics adoptent des politiques en matière de témoins de connexion, il est vrai que ces derniers doivent tout de même divulguer des informations spécifiques sur l'utilisation des renseignements qu'elles collectent y compris celles qui sont collectés par des témoins.
Le projet de règlement impose l'obligation pour les organismes publics de publier une politique de confidentialité ainsi qu'un avis pour toute	La notion de confidentialité n'est qu'une partie des obligations légales des organismes publics en ce qui concerne le traitement des renseignements

modification ultérieure. L'objectif de cette démarche est d'offrir aux utilisateurs une plus grande transparence et de créer une harmonisation au sein du système de traitement des données par les organismes publics. L'objectif est alors d'accroître la transparence. Cependant, il convient de noter que des lacunes persistent, comme étudier article par article ci-dessous. Ces manquements entravent une totale transparence. D'autre part, l'objectif d'harmonisation peut susciter des questionnements quant à la pertinence de sa réalisation. La distinction entre les secteurs public et privé perdure, et cette différence peut influencer la mise en place de mesures harmonisées. De plus, certains éléments essentiels à une politique de confidentialité ne sont peut-être pas exhaustivement référencés, entraînant un manque de force obligatoire. Cette flexibilité laissée aux organismes publics pourrait entraver la volonté d'atteindre l'harmonisation voulue. En résumé, le projet de règlement exige la publication de politiques de confidentialité et d'avis de modification pour les organismes publics, visant à renforcer la transparence et à harmoniser leur système de traitement des données. Néanmoins, les insuffisances et manquements peuvent limiter cette transparence. Certains éléments pouvant sembler essentiel à la bonne compréhension du traitement des données ne sont pas imposé. Cela laisse aux organismes une certaine liberté rédactionnelle qui nuit à l'harmonisation complète des politiques de confidentialité.	personnels. En effet, il faut ajouter le volet d'accès à l'information, mais aussi la protection de l'intégrité des renseignements et la disponibilité de ceux-ci. L'article 19 de la LCCJTI est éclairante à ce sujet : « Toute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné. » Il serait donc plus à propos de parler de politique sur l'accès et la protection des renseignements personnels plutôt que de politique de confidentialité. De plus, il ne semble pas y avoir de motif valable de limiter la portée du règlement aux renseignements recueillis à l'aide d'un moyen technologique. L'article 1 de la *Loi sur l'accès* énonce clairement que la loi s'applique « quelle que soit la forme de ces documents : écrite, graphique, sonore, visuelle, informatisée ou autre », et non seulement aux renseignements recueillis par un moyen technologique.
L'article 63.4 de la Loi sur l'accès prévoit qu'un organisme public qui recueille par un moyen technologique des renseignements personnels doit publier sur son site Internet et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs. Le projet de règlement découlant de cet article sert à établir le contenu et les modalités de la politique et de l'avis de changement pour concrètement harmoniser le contenu des politiques de confidentialité des organismes publics et permettre aux citoyens de comprendre leurs droits et de quelle façon leurs renseignements personnels sont recueillis et utilisés. Le projet de règlement remplit sans aucun doute son premier objectif en lien avec une meilleure harmonisation notamment en énonçant le contenu minimal de toute politique de confidentialité à l'article 2 ainsi que de tout avis de modification à l'article 4. Toutefois, le deuxième objectif en lien avec une meilleure compréhension du public est rempli que partiellement. Effectivement, les articles 6 et 7 du projet de règlement émettent des balises quant à	L'objectif du législateur étant de déterminer le contenu et les modalités des politiques de confidentialité des organismes publics et d'harmoniser ce contenu en le rendant plus accessible pour les citoyens, selon moi, les dispositions manquent une certaine portée afin de réellement atteindre leur objectif. En effet, certains aspects cruciaux devraient se retrouver dans le projet de règlement. D'abord, l'objectif d'uniformisation me semble difficile à atteindre. Bien que les organismes aillent se conformer à ce règlement, l'uniformisation aux yeux des citoyens ne se fera pas pour autant. Selon moi, cette uniformisation pourrait se faire si non seulement les critères devant s'y retrouver sont présents, mais aussi **la manière** dont ils sont présentés dans chaque politique. Cela rendrait le tout plus cohérent pour le commun des mortels. L'objectif visant à rendre les informations plus accessibles pour les citoyens me parait également non atteint considérant les articles présentés dans le projet. En effet, selon moi, la personne raisonnable n'ayant pas de connaissances en matière de renseignement personnel aura de la difficulté à

la publicisation de la politique de confidentialité et de l'avis de modification pour s'assurer que le public en prenne connaissance. Toutefois, il n'y aucune stipulation portant sur le caractère compréhensible de ces documents par la rédaction en des termes simples et clairs (par exemple, en exigeant le plus possible l'incorporation de tableaux ou de résumés et l'utilisation d'un langage inclusif pour les personnes présentant un faible degré de littératie).	bien saisir la portée du contenu d'une politique de confidentialité respectant les exigences du Règlement. Prenons en exemple l'art. 2(10) du Règlement qui indique que la politique devra avoir une mention quant à la possibilité que le renseignement personnel soit utilisé à l'extérieur du Québec. Il devrait selon moi y avoir des exemples concerts permettant au citoyen de bien saisir dans quels contextes leurs renseignements pourront être communiqués afin d'atteindre un consentement valide.
Le projet de règlement, à travers son champ d'application, son contenu et ses différents articles, permet de favoriser une structure uniforme des politiques de confidentialité des organismes publics. De plus, à mes yeux, il permet aux citoyens de s'informer suffisamment afin d'être habilité à consentir de manière éclairé à la collecte de leurs renseignements personnels. Toutefois, même si la rédaction du projet de règlement est de qualité, je n'accorderais pas la note parfaite, en considérant que certains éléments dans le contenu, pourrait être modifiés ou ajoutés. Un exemple, est la sécurité des renseignements personnels dans un contexte numérique, qui est mise de l'avant, dans le projet de règlement, à travers les nouvelles structures de protection instaurées par la *Loi 25*, tel que le responsable de la protection des renseignements personnels de l'organisme public, le comité sur l'accès à l'information et la protection des renseignements personnels et le processus de traitement des plaintes relatives à la protection des renseignements personnels. Toutefois, à l'article 2, alinéa 1, paragraphe 11, du projet de règlement, on exige seulement « une brève description des mesures » de sécurité, ce qui à mes yeux, devrait être plus précis afin d'exiger de nommer les mesures physiques, administratives et techniques concrètes afin de rassurer les citoyens sur la protection des renseignement personnels, et ce sans pour autant mettre l'entreprise à risque d'attaque au niveau des données personnels.	Le projet de règlement énonce l'objectif d'harmoniser les politiques de confidentialité des organismes publics, afin de permettre aux citoyens d'obtenir les informations nécessaires pour comprendre leurs droits et mieux saisir le traitement de leurs renseignements. Or, la portée du projet de règlement se limite aux organismes publics qui recueillent ces renseignements par moyen technologique. La *Loi sur l'accès* n'exige pas de politique hormis ce cas, entraînant une portée assez restreinte du règlement. Une portée plus adéquate (et plus neutre technologiquement) inclurait donc la collecte de renseignement « par tout moyen » à l'article 63.4 *Loi sur l'accès*, emportant une application plus globale du règlement. Le champ d'application du règlement comporte une autre lacune. Afin d'harmoniser le contenu des politiques adressées au public, il aurait été pertinent d'y assujettir les entreprises (*Loi sur le secteur privé*) (voir 2.1). Il faut aussi noter l'absence de règles relatives aux technologies de suivi (témoins de connexion sont exclues de l'article 63,7 *Loi sur l'accès*, laissant un potentiel vide juridique). Il aurait été pertinent d'adresser cette considération, toujours dans une perspective de renseigner le citoyen, puisqu'une politique sur les témoins de connexion va souvent de pair avec la politique de confidentialité (bien qu'elles puissent être consignées sur des pages séparées). Le citoyen qui souhaite se renseigner sur l'utilisation de ses données personnelles peut certainement s'intéresser aux cookies, notamment quant à l'impact de leur utilisation (essentiels/non-essentiels). Comme il s'agit d'une information qui se présente bien sous forme de tableau, l'ajout d'un article pourrait l'exiger ainsi.

1.4 Pensez-vous que ce projet de règlement peut être appliqué concrètement et qu'il est réaliste ? Anticipez-vous des conséquences négatives découlant des orientations présentées, et, si oui, lesquelles ?

D'abord, il est certain que la date d'entrée en vigueur arrive rapidement. En effet, l'article 63.4 de la LAI entre en vigueur le 22 septembre 2023, et le projet de règlement entre ensuite en vigueur	Je crois que l'application du Règlement sera assez difficile à mettre en pratique. L'entrée en vigueur de la Loi 25 arrive déjà assez vite, ce qui fait en sorte que les organismes publics n'ont pas

le 1e janvier 2024. Donc, en peu de temps, les organismes publics devront s'y conformer. Aussi, au-delà de la rédaction d'une politique de confidentialité conforme au projet de règlement, les organismes devront en faire la mise à jour régulièrement. Il est certain que cela peut nécessiter un investissement en temps et en ressources significatives, ce qui peut être un gros changement pour certains organismes. Malgré tout, je pense que le projet est réaliste, car il donne des balises claires aux organismes afin d'améliorer leurs pratiques en matière de gestion des renseignements personnels. En revanche, un impact négatif qui pourrait possiblement découler de ce projet de règlement serait le découragement des organismes publics de recueillir des renseignements personnels par moyens technologiques, étant donné qu'ils sont assujettis à des obligations plus précises que les organismes publics qui font une collecte verbale. En effet, ces derniers doivent uniquement informer la personne concernée sur ses pratiques de gestion des renseignements personnels, lors de la première collecte, et par la suite, sur demande (article 65 LAI). D'ailleurs, les informations à fournir sont moins précises et détaillées que pour le contenu de politique de confidentialité d'un organisme public faisant la collecte par moyen technologique.	beaucoup de temps pour s'y conformer. Je crois que la même situation se reproduira pour le règlement : en septembre 2023, les organismes publics auront tout juste terminé de se plier aux exigences de la Loi 25 et devront ensuite se dépêcher à ajuster leurs politiques de confidentialité pour janvier 2024 (la qualité en sera peut-être affectée). Le second élément qui m'inquiète par rapport à la mise en application est la collecte commune de renseignements personnels faite par les organismes publics. Il s'agit d'un concept qui me semble plutôt flou et j'ai de la difficulté à concevoir comment le tout va se déployer dans la pratique. Dans le cas d'un incident de confidentialité, il me semble qu'il va être difficile d'attribuer la responsabilité à un seul organisme si la collection est commune. Aussi, ce type de collecte ne pourrait-il pas présenter un plus grand danger d'incident ? Si un organisme public recueille des renseignements personnels au nom d'autres organismes publics, et qu'une seule entité est à l'origine de toutes les collectes, on pourrait arguer qu'il est plus facile d'y créer une faille. L'incident potentiel touchera aussi une bien plus grande quantité de renseignements et conséquemment, d'individus. On pourrait alors faire face à plusieurs litiges compliqués.
Je suis d'avis que certaines exigences ne sont pas réalistes ou du moins auront des répercussions négatives puisque certaines d'entre elles alourdissent le travail des organismes publics. Par exemple, obliger que toute modification à la politique, que celle-ci soit cléricale ou significative, fasse l'objet d'un avis de modification augmente inutilement le fardeau des organismes publics. De plus, l'organisme public risque de recourir au comité sur l'accès à l'information et la protection des renseignements personnels en surabondance puisque les types de modifications qui doivent faire l'objet d'une consultation auprès dudit comité manquent de clarté. Obliger les organismes publics à fournir dans leur politique de confidentialité les coordonnées du responsable de la protection des renseignements personnels et les coordonnées de la personne, de l'organisme concerné ou d'une unité administrative à qui toute question relative à cette politique peut être soumise est contre-productif et risque d'avoir pour effet de dédoubler le travail, car la personne qui souhaite communiquer avec l'organisme public risque de contacter les deux personnes-contacts fournies dans la politique quitte à être répondue le plus rapidement possible. Je suis également d'avis que le projet de règlement tel que rédigé n'assure pas le même niveau de clarté pour toutes les	Le projet de règlement est généralement réalisable. Premièrement, les exigences minimales concernant le contenu des politiques de confidentialité (article 2) ainsi que des avis de modification (article 4) sont claires et raisonnables. Deuxièmement, les obligations concernant les manières de publicisation (articles 6 et 7) ne sont pas trop contraignantes et permettent d'imposer aux organismes un certain devoir de transparence envers les citoyens par la facilitation de la communication de leur politique de confidentialité et des avis de modification. Toutefois, à l'article 4, il est demandé aux organismes publics d'émettre un avis dans un délai de 15 jours pour toute modification, qu'elle soit significative ou non, apportée à une politique de confidentialité. Il s'agit ici d'une obligation beaucoup trop contraignante pour les organismes qui devront, par exemple, émettre un tel avis dans le délai requis s'ils souhaitent changer la syntaxe d'une phrase. Bien que cette disposition souhaite prôner une meilleure transparence envers le public, ce serait plutôt le comportement inverse qui se propagerait chez les organismes publics. Effectivement, pour tenter d'esquiver le lourd fardeau qui leur est imposé, il sera préféré de ne pas apporter de modifications aux politiques de confidentialité, ou très peu, plutôt que de les

politiques de confidentialité. Certaines politiques de confidentialité risquent d'être plus claires et plus faciles à lire du fait que le projet de règlement n'encadre pas le format et la structure de la politique de confidentialité.	mettre à jour régulièrement. Cela risquerait notamment de mettre en péril l'évolution des droits des personnes concernées en favorisant des politiques figées dans le temps.
Le règlement prévoit des exigences claires et détaillées pour les politiques, la consultation préalable, la publication de la politique et les avis de modification. À mon avis, tout cela est un bon signe du réalisme du règlement. Je pense que la mise en œuvre au début ne posera pas de problème. Les exigences ne me semblent pas trop élevées, puisque les organismes ont essentiellement simplement besoin de bâtir leur politique conformément aux normes établies par le règlement et d'ensuite la rendre facilement accessible sur leur site web. Cependant, je n'écarte pas la possibilité que l'application dans le temps pourra causer des problèmes. Plus particulièrement pour ce qui a trait aux avis de modification. Je trouve qu'il y a une lacune à cet égard, puisqu'on ne distingue pas la procédure à suivre pour des modifications de nature cléricale versus de nature substantielle. Je traiterai plus tard des notions du délai de 15 jours, mais je pense qu'il importe de soulever que la consultation auprès du comité sur l'accès à l'information pour toute modification semble superflue. Concrètement, ça représente énormément de temps et de ressources qui devront être alloués pour analyser les modifications, alors que certaines d'entre elles ne méritent sans doute pas l'attention d'un comité. On sait déjà que de nombreux délais sont associés avec l'utilisation des services d'organismes publics et cette exigence du règlement n'améliorera pas les choses. Bref, il faudrait qu'une distinction soit faite entre les modifications de substance qui affectent le consentement des utilisateurs et les autres modifications.	La quantité de nouvelles obligations liées à la mise en place de ce projet de règlement pourrait rendre son application ardue et irréaliste, du moins dans les premiers temps de sa mise en vigueur. En effet, les organismes doivent être en mesure de se conformer à plusieurs nouveautés (contenu de la politique de confidentialité, comité sur l'accès à l'information et la protection des renseignements personnels, responsable de la protection des renseignements personnels), ce qui rend complexe l'application du projet de règlement. Des difficultés pratiques liées à son application peuvent également s'ajouter. Par exemple, l'obligation pour l'organisme de transmettre les coordonnées de la personne responsable de répondre aux questions relatives à la politique (art. 2(13) projet de règlement) entraine beaucoup plus d'organisation à l'interne qu'une simple transmission de coordonnées. Il s'agit de mettre en place un mécanisme complet de service à la clientèle efficace. Ainsi, le projet de règlement ne semble pas être irréaliste ou irréalisable sur le long terme, mais il faut prévoir une période d'adaptation afin, non seulement que les organismes puissent s'y conformer, mais également que le tout soit fonctionnel permettant l'atteinte des effets désirés. De plus, le contrôle de la conformité du projet de règlement semble difficile à réaliser. En effet, comment assurer que tous respectent le règlement ? Comment assurer que le contenu des politiques soit juste et complet ? De mauvaises politiques de confidentialité impactent directement les consommateurs et peuvent leur être préjudiciables, ceux-ci ne recevant pas toute l'information nécessaire.
Tel quel, le projet de règlement ne peut pas être appliqué car il y a un grand manque d'informations quant aux mesures de sécurité qui ne permettent pas d'avoir un consentement éclairé des utilisateurs. Toutefois, le projet de règlement est réaliste dans l'optique où de telles mesures ont déjà été prises par d'autres autorités telles que le fédéral qui a établi des normes requises pour la création de politiques de confidentialité par l'entremise de la LPRPDE. L'ensemble des entreprises privées dans le reste du Canada (excepté la C-B et l'Alberta qui détiennent leur propre loi) se doivent de se conformer à cette loi. Cela permet une plus grande transparence pour les utilisateurs	De mon point de vue, la mise en place du projet de règlement ne sera pas sans difficulté, car il impose des exigences considérables. Cette situation pourrait entrainer des défis particuliers pour les organismes publics qui ont des ressources plus limitées, comme les municipalités (Journal des débats, 2020). Un exemple évident de ces difficultés est l'instauration d'un comité sur l'accès à l'information et la protection des renseignements personnels qui devra être consulté avant de publier la politique de confidentialité et les avis de modifications. Cette démarche sera très couteuse en temps et en argent pour ces organisations. Un autre aspect qui pourrait susciter des défis en pratique est

concernant l'usage de leurs renseignements personnels. En contrepartie, une des conséquences négatives possibles serait que les organismes publics ne sont pas prêts à appliquer cette politique de confidentialité compte tenu de la structure qui doit être mise en place pour respecter la confidentialité des renseignements personnels. Des changements informatiques devront être implantés pour maintenir les nouvelles règles de sécurité des renseignements et historiquement, les organismes publics ont connu des ratés en lien avec la modernisation du système (plusieurs attaques informatiques, système inadéquat tel que Phénix). Il y a également plusieurs questionnements concernant la préparation des organismes publics quant à leurs mesures de sécurité considérant la nature des renseignements personnels qui varie d'un organisme à un autre. Par exemple, les mesures d'anonymisation des renseignements personnels à la fin de leur usage en respect avec la loi.	l'avis de modification. Selon la version actuelle du projet de règlement, un avis de modification devra être publié 15 jours avant tout changement dans la politique de confidentialité, à moins d'avis contraire. En pratique, une organisation pourrait se retrouver dans la nécessité de faire plusieurs modifications à sa politique de confidentialité, et ce, même à l'intérieur d'un délai de 15 jours. Il devient alors difficile pour l'organisation de maintenir la politique à jour. Enfin, les exigences minimales, qui sont en réalité assez exigeantes quant au contenu de la politique de confidentialité, pourraient mener à des conséquences négatives. En effet, pour satisfaire ces exigences, les organismes pourraient être menés à créer des politiques excessivement longues ce qui rajoute un fardeau sur les épaules de l'usager qui veut comprendre ce document.
L'article 8 du projet de règlement affirme de celui-ci devrait entrer en vigueur le 1er janvier 2024. Cependant, l'article 63.4 de la *Loi sur l'accès*, demandant que les organismes publics publient une politique de confidentialité entrera lui en vigueur le 22 septembre 2023. Ainsi, entre le 23 septembre et le 31 décembre 2023, les politiques de confidentialité devront être publiées, mais les exigences concernant ce qui doit être inclus dans celle-ci ne seront toujours pas établies. Cela est d'autant plus grave puisque des commentaires peuvent encore être envoyées concernant le projet de règlement, jusqu'au 45e jour suivant le 12 juillet 2023. Il est toujours possible que des modifications soient apportées au projet de règlement et donc, que les organismes publics ayant déjà travaillé sur leur politique de confidentialité doivent la modifier à nouveau. Il s'agirait donc de demander aux organismes publics d'utiliser beaucoup de ressources pour rédiger et corriger leurs politiques à ces deux dates. Je considère que cela pourrait causer une grande confusion chez les citoyens. En effet, si les citoyens voient une première politique de confidentialité en septembre 2023, et en voient une nouvelle dès janvier 2024, cela pourrait mener à une mauvaise compréhension de quels renseignements seront recueillis et/ou comment ceux-ci seront utilisés. Je considère que les changements fréquents pourraient diminuer la confiance du public, envers les organismes publics concernant la protection des	Après l'analyse de ce règlement, je crois que certains articles sont réalistes et que d'autres sont un peu plus difficiles à appliquer en pratique. Concernant l'avis de modification, je peux envisager certaines difficultés d'application en pratique. Plus précisément, l'article 5 du projet de règlement indique que tout avis de modification concernant une modification significative à une politique doit faire l'objet d'une consultation auprès du comité sur l'accès à l'information et la protection des renseignements personnels, et ce, avant d'être publiée. De nos jours, nous savons que la technologie évolue très vite et qu'il est parfois difficile de s'adapter rapidement aux changements. Par exemple, admettons que de grands changements informatiques viennent bouleverser la façon de collecter les renseignements personnels et que plusieurs organismes publics souhaitent modifier substantiellement leur politique de confidentialité en même temps, l'obligation de révision de l'avis de modification par le CAI peut s'avérer être une tâche lourde et longue d'autant plus qu'il n'y a pas de précision dans le règlement sur ce que peut être une « modification significative ». Bien qu'il s'agisse d'une bonne initiative, je peux anticiper certaines conséquences négatives de cette disposition. En ce qui a trait à l'article 3 du projet de règlement, je pense que la collecte commune de renseignements personnels peut entraîner certaines difficultés au niveau de l'obtention du consentement des personnes concernées ainsi qu'au niveau de la responsabilité

renseignements personnels, alors qu'il s'agit d'un sujet qui a causé beaucoup d'angoisse dans les dernières années.	de l'organisme dans un cas d'incident de confidentialité (voir 2.3).
Il semble peu réaliste de penser que l'ensemble des organismes publics se conformera dans les délais prévus par la Loi. D'abord, si la Commission d'accès à l'information (CAI) a mis en place des mesures d'accompagnement pour aider les entreprises privées à se conformer aux nouvelles dispositions de la Loi 25, elle ne semble pas mettre la même énergie à accompagner les organismes publics (voir le dernier rapport de gestion annuel de la CAI, p.45). Or, il serait souhaitable que la CAI émette des lignes directrices et autres documents d'accompagnement pour les organismes publics afin de les aider dans cette transition. De plus, les incitatifs ne sont pas nombreux dans le secteur public. En effet, si la Loi 25 augmente les amendes prévues pour diverses infractions commises par les organismes publics, celles-ci restent dérisoires par rapport aux sanctions applicables aux entreprises privées. L'effet persuasif en est affaibli. En ce qui concerne les organismes publics, le risque est plutôt d'ordre réputationnel, la conséquence étant la perte de confiance des citoyens.	Comparé à la législation appliquée au secteur privé, avec de grandes responsabilités sur les entreprises, les directives de cette réglementation semblent plus simples à mettre. Cette simplicité d'application est un atout majeur, permettant une mise en pratique facilitée, sans trop de contraintes. Cependant, ce niveau modéré de mentions obligatoires peut engendrer des problèmes lors de la mise en œuvre, en raison d'un manque de précision dans le règlement. Malgré leur faisabilité, ces obligations rencontrent des difficultés dans leur application. Les manquements, tels que la destruction ou la collecte de données sur les mineurs, posent des problèmes complexes à résoudre, pouvant entraîner des conséquences graves. De plus, la notification des avis, bien que considérée comme essentielle, peut se heurter à des obstacles lors de sa mise en place. Les procédures et les moyens pour notifier efficacement les utilisateurs peuvent se révéler compliqués. Ainsi, bien que cette réglementation puisse sembler moins contraignante que les lois du secteur privé, sa simplicité d'application peut présenter des défis substantiels. Les problèmes liés aux manquements, à la protection des mineurs et à la mise en œuvre des avis montrent que des aspects pratiques doivent être soigneusement étudiés pour garantir une application efficace et éthique de ces obligations.
Je considère que ce projet de règlement comporte des enjeux à considérer au niveau de sa mise en application. Je suis d'avis que ce projet de règlement, dans son entièreté actuelle, sans modification, pourrait être difficile à adopter sans mener à des incohérences au niveau de l'uniformisation des politiques de confidentialité en raison des différentes problématiques soulevés dans cette analyse. Toutefois, je considère que certains éléments, tel que le contenu minimal des politiques de confidentialité, abordé à l'article 2 du projet de règlement, permettra de servir de guide pratique pour les organisations publics afin de répondre et se conformer aux différentes exigences législatives applicables au secteur public dans la *Loi sur l'accès*. De plus, il faut tenir compte que les organisations publics font actuellement face à un défi considérable, en lien avec la préparation et mobilisation nécessaire afin de se conformer, aux nouvelles exigences en matière de protection à la vie privée, en raison de l'entrée en vigueur de la *Loi 25*, le 22 septembre 2023. En ce sens, à mes yeux, il me semble	Selon moi, ce projet de Règlement, bien qu'il comporte des objectifs pertinents et nobles, n'est pas réaliste. Afin que ce règlement soit appliqué concrètement et d'une manière adéquate, il faudrait ajouter de nombreuses clarifications quant à la portée de chaque article. Commençons par l'objectif d'harmonisation des politiques de confidentialité pour le citoyen. Dès le préambule, le Règlement n'est pas clair et le texte ne réussit pas à amener les nuances nécessaires pour clarifier le tout. Par harmonisation, le législateur entend-il uniformiser les sites Internet partout au Québec ? Ou compte-t-il uniformiser le type d'information se retrouvant dans les politiques ? Peu importe son intention, le projet ne permet pas d'atteindre cet objectif. En effet, il est improbable que chaque organisme public réponde aux exigences d'une manière similaire. Prenons en exemple l'art. 2 (10) et (11). L'utilisation des expressions « une mention » et « brève description » laisse selon moi trop de place à interprétation et aux conséquences négatives. Selon moi, une simple « mention » de la

important de considérer que l'application de ce nouveau règlement s'avérera particulièrement ardue et peu réaliste au niveau opérationnel et des ressources humaines pour ces organisations publics.	possibilité que les renseignements personnels soient utilisés à l'extérieur du Québec n'apporte pas assez de précision à l'utilisateur. L'organisme pourrait utiliser cette disposition pour cacher certaines utilisations faites avec les renseignements personnels. De plus, le consentement de l'utilisateur se voit affecté par ce manque d'informations pertinentes. L'ajout d'une annexe comportant des exemples d'informations devant sur retrouver dans la politique de confidentialité permettrait une application plus concrète du Règlement, permettant d'approcher l'objectif d'harmonisation (sans toutefois l'atteindre).
Le projet suscite des enjeux quant au principe de démontrabilité, qui exige des organismes qu'ils soient en mesure de démontrer leur conformité à la loi. Les organismes ont l'obligation de porter la politique à l'attention de la personne concernée, en plus d'être publiée sur le site Internet de l'organisme (art. 6 et 7). Sans plus de détails, il s'avère difficile pour l'organisme de démontrer s'être acquitté de ses obligations : dans quelle mesure démontrer qu'une politique publiée a été portée à l'attention du citoyen ? Est-ce de façon à obtenir un consentement valide ? L'individu doit-il consentir à la politique ? Il pourrait être intéressant de remanier l'article 7 pour clarifier les exigences qui y sont liés. En effet, les organismes auraient intérêt à avoir une obligation plus claire pour mieux s'y conformer. Il pourrait être question de rendre la politique *accessible* avant que l'individu ait recours aux services de l'organisme ou lorsque cet individu s'apprête à fournir des renseignements. Selon le WP29, *l'accessibilité* à une politique comprends la possibilité pour l'individu de prendre connaissance des principales conséquences du traitement des renseignements personnels, ainsi que les droits et les mesures de sécurité afférents (par. 10). L'article 5 manque aussi de précision. Il est difficile de démontrer que la politique de confidentialité a fait l'objet d'une « consultation » auprès du comité d'accès à l'information. Il est possible de renforcer cette obligation en exigeant l'approbation du comité. Une mention à cet effet sur la politique (art. 2) peut suffire pour en assurer le public.	Certains éléments du projet ne semblent pas réalistes. Concernant les catégories de personnes qui ont accès aux renseignements personnels, il peut être difficile d'en établir une liste. Par exemple, concernant les structures hospitalières, si une grande majorité du personnel a accès à certaines données personnelles telles que les noms et prénoms, seule certains employés auront accès à d'autres données sensibles telles que les données biomédicales. Comme proposé ici, l'utilisateur pourrait difficilement distinguer et comprendre qui a accès à quoi. Peut-être pourrions nous proposer une distinction entre les types de données personnelles, telles que les données à caractère administratif et les autres données (biomédicale, biométriques…) en établissant un tableau type. Il serait aussi nécessaire d'établir quels sont les renseignements qui seront partagés avec quel établissement. Le fait que les organismes publics peuvent recueillir des informations en commun pour le compte de plusieurs organismes publics nous semble problématique. La question du consentent de l'utilisateur se pose, il doit être exprès, donc l'utilisateur doit valider que ses données soient partagées avec un ensemble d'organismes publics. Ceci ne semble pas permettre que l'utilisateur consente à donner certains renseignements à certains organismes et pas à d'autres. La question de la nécessité se pose : les fins de chaque organisme public sont potentiellement différentes, ainsi les informations ne devraient pas être toutes partageables. En cas de faute, lorsque la collecte d'informations dépasse les fins nécessaires, se pose la question de la responsabilité entre l'organisme collecteur et l'organisme profitant de cette collecte.

1.5 Le format du projet de règlement est-il adapté et en facilite-t-il la consultation ? Le texte est-il suffisamment clair ?

Dans son ensemble général, le projet de règlement est quand même clair et concis même si ce dernier pourrait avoir besoin de quelques ajouts. En effet, il est certain que les 8 articles qui constituent ce règlement en facilitent la consultation pour les organismes publics. Toutefois, un règlement succinct ne veut pas nécessairement dire que certains articles n'ont pas besoin de précisions supplémentaires afin de ne rien laisser au hasard ou bien à l'interprétation large des organismes publics. Plus précisément, les articles 3, 4 et 6 auraient besoin d'un peu plus de détails (voir 2.3, 2.4. et 2,5.). Au niveau des termes utilisés, je suis d'avis que le contenu du règlement a été rédigé en fonction des connaissances d'une personne raisonnable et que le vocabulaire employé est compréhensible et précis. Afin que le contenu du règlement soit plus clair, des exemples pourraient être ajoutés au règlement en faisant la mention de « notamment » dans une disposition pour énumérer certains cas qui peuvent s'appliquer en l'espèce sans que cette énumération soit restrictive. Par exemple, à l'article 2 (paragraphe 2) : « une description des renseignements personnels recueillis, notamment : le nom, l'adresse courriel, le numéro de téléphone, etc. ». Certaines énumérations pourraient, entre autres, mieux encadrer et guider les organismes publics dans la rédaction de leur politique de confidentialité.	Je suis d'avis que certaines sections du projet de règlement manquent de clarté et sont sujettes à interprétation. À titre d'exemple, l'article 5 du projet de règlement prévoit que tout avis de modification concernant une modification significative à une politique doit, avant d'être publié, faire l'objet d'une consultation auprès du comité sur l'accès à l'information et la protection des renseignements personnels. Le manque de clarté autour de l'expression « modification significative » peut conduire les organismes publics à adopter une approche plus conservatrice de sorte que les organismes publics recourront inutilement ou en surabondance le comité sur l'accès à l'information et la protection des renseignements personnels. L'article 7 du projet de règlement manque également de clarté en ne précisant pas le moyen pour porter la politique à l'attention de la personne concernée par les renseignements personnels recueillis par un moyen technologique. Serait-ce suffisant de diriger les personnes concernées vers le site internet de l'organisme public ?
Le projet de règlement est plutôt clair. Il utilise des termes simples, et qui peuvent être pris dans leur sens commun. De ce fait, le public qui consulte le projet de règlement devrait être capable de le comprendre sans trop de difficulté. Le préambule aide à déterminer l'objectif du règlement et à comprendre les lois habilitantes qui ont menés à sa conception. En effet, le préambule permet de comprendre dans quel cas ce projet devra être respecté, et à quoi ils devraient s'attendre à la lecture d'une politique de confidentialité. Une première difficulté, cependant, se remarque au premier article, soit dans le terme « organisme public ». En effet, la définition d'organisme public peut être particulièrement difficile à interpréter. Les articles 3 à 7 de la *Loi sur l'accès* viennent expliquer à quels organismes le projet de règlement s'applique, mais posent aussi plusieurs exceptions qui rendent la compréhension de ce terme plus complexe. Une deuxième difficulté provient du fait que ni dans le projet de règlement et ni dans sa loi habilitante pouvons-nous trouver	À mon avis, le format du projet de règlement est suffisamment clair. Il s'agit d'un format traditionnel de projet de règlement que l'on retrouve sur le site de la *Gazette officielle du Québec*. Il est très court et comporte cinq divisions distinctes dans un enchaînement logique des idées. Le langage est aussi simple et clair à comprendre, car il n'y a pas de jargon juridique difficile à comprendre. En revanche, la section III, concernant l'avis de modification, pourrait à mon avis, être divisée en deux articles, soit l'un stipulant le délai, et l'autre stipulant les exigences de l'avis, pour favoriser le principe d'une idée par phrase. Aussi, il est pertinent de mentionner que la CAI a le pouvoir d'élaborer des lignes directrices (2022, lien). Je crois que telles lignes directrices sont essentielles pour vulgariser et traduire l'esprit et l'objectif d'une loi ou d'un règlement pour en faciliter l'application. La CAI a déjà publié un projet de lignes directrices sur le consentement (2023-1), qui contient quelques recommandations de rédaction d'une politique de confidentialité (2023, lien). La rédaction de lignes

une définition de ce qu'est un renseignement personnel. La définition québécoise est inscrite à l'article 2 de la *Loi sur la protection des renseignements personnels privés*. Le terme « renseignement personnel » est utilisé à maintes reprises dans le projet de règlement, mais aucun renvoi ou aucune mention à cette définition ne s'y trouve. Je considère que cela peut mener à confusion sur ce qui est ou n'est pas collecté par les organismes publics.	directrices reste toutefois à la discrétion de la CAI. Notons que le Commissariat à la vie privée du Canada a aussi publié dix conseils pour améliorer les politiques de confidentialité (novembre 2018, lien). En bref, le projet est suffisamment clair. Il est bien structuré et comporte un enchaînement logique des idées, le rendant adapté pour la consultation. Assorti de lignes directrices, l'objectif poursuivi par le projet sera atteint encore plus rapidement.
Dans l'ensemble, le règlement est bien adapté aux organismes publics. Il est bien structuré grâce aux sous-titres qui séparent les exigences pour la politique de confidentialité de celles pour l'avis de modification et qui prévoient une section qui réunit les exigences pour ces deux types de documents. De plus, le langage utilisé est relativement simple, ce qui facilite la lecture. Cependant, quelques améliorations auraient pu être adoptées. Il aurait été pertinent d'inclure dans le règlement des définitions de certains concepts qui ne sont pas décrits dans la *Loi sur l'accès* telles que la « modification significative » ou encore le principe de « collecte commune » pour faciliter la compréhension du lecteur. Aussi, l'article 2 est particulièrement long et aurait pu être simplifié en regroupant l'information qu'on souhaitait retrouver dans la politique de confidentialité en catégorie plutôt que d'énumérer chaque élément. Il aurait pu, par exemple, se baser sur le modèle de la politique de l'article 65 de la *Loi sur l'accès* et l'adapter à son contexte. Par ailleurs, à mon avis, l'article 4 a une formulation qui peut être complexe à suivre. Il aurait été plus simple pour le lecteur de changer la tournure de phrase pour indiquer qu'il doit y avoir un avis de modification au moins 15 jours avant de modifier la politique. Enfin, l'ajout d'une annexe proposant un exemple de politique de confidentialité aurait pu être bénéfique. Cela permettrait d'offrir aux organismes un modèle à suivre, les aidant à mieux comprendre à quoi s'attendre et à rédiger leur politique efficacement.	Le texte est général et n'apporte aucun détail pour la consultation. Le but de ce projet de loi consiste à définir des paramètres aux politiques de confidentialité pour que les utilisateurs soient informés de l'usage de leurs renseignements, et donc de leurs droits en regard à leur vie privée. Toutefois, le texte apporte peu de clarification sur le traitement de ses renseignements personnels, soit au niveau du consentement ou aux mesures de sécurité applicables selon le degré de sensibilité des renseignements. De plus, le texte n'a pas un niveau du langage courant pour permettre aux utilisateurs de bien le comprendre. Une solution pour faciliter la consultation serait de publier un résumé des modalités sur les sites internet des autorités compétentes ou faire une diffusion plus large dans les médias pour vulgariser la réglementation. Des tableaux avec des titres clairs concernant le traitement des renseignements permettraient de rendre les indications plus visibles et accessibles à tous. Aussi, bien que le projet de loi soit publié à la Gazette Officielle du Québec selon les normes de publication, une version accessible pour tous, par exemple par courriel ou affichée par les organismes publics concernés, permettrait à plus de personnes d'y avoir accès et donc de prendre en considération cette nouveauté dans la loi. De plus, une foire aux questions qui explique bien les paramètres de ce règlement déposée au même endroit que le règlement permettrait aux personnes concernées de bien comprendre un tel règlement pour la protection de leur vie privée.
Je crois que le format du projet de règlement est assez adapté. Les sections sont claires et le règlement est concis, ce qui permet aux organismes publics de rapidement repérer ce dont ils ont besoin. En revanche, je changerais les noms des sections dans un esprit de précision, afin qu'il soit facile de reconnaître de quoi il est question dans cette partie. Par exemple, la Section IV pourrait devenir « Publicisation d'une politique de confidentialité et d'un avis de modification ». Autrement, quelques passages ont attiré mon attention en raison du fait qu'ils	La brièveté de ce texte le rend aisément compréhensible, offrant une clarté immédiate. Cependant, sa concision a pour conséquence l'omission de certaines informations essentielles. Malgré son format compact qui favorise la consultation, le texte ne renforce ni la protection des données ni la clarté dans leur traitement. Certains termes pourraient sembler obscurs, mais il convient de rappeler que le texte est destiné aux organismes publics concernés. Puisqu'il soit concis, il se limite à l'obligation de publier une politique de consentement et ses modifications

pouvaient éveiller certaines ambiguïtés. À l'article 3, 2e alinéa, il est énoncé qu'une politique de confidentialité peut être commune à plusieurs organismes publics « dans la mesure où ils recueillent en commun des renseignements personnels. » Toutefois, qu'est-ce qui se qualifie comme une collecte commune ? Comment procéder pour qu'il soit considéré que des renseignements personnels ont été recueillis communément ? Ensuite, l'article 7 du Règlement stipule que la politique de confidentialité et l'avis de modification, dans le cas d'une collecte par moyen technologique, « doivent être portés à l'attention de la personne concernée par ces renseignements. » Mais de quelle manière ? Si le Règlement poursuit un objectif d'harmonisation, il pourrait être beaucoup plus facile de simplement uniformiser la pratique en spécifiant la méthode qui pourrait être utilisée pour les porter à l'attention de la personne (ex. un bandeau sur le site Internet de l'organisme public, Mémoire au Conseil des ministres).	sans aborder davantage de détails. Pour combler ce manque, il serait envisageable de mettre en place des outils tels que des lignes directrices, similaires à celles du secteur privé, bien que cela ne garantisse pas nécessairement une plus grande clarté. Les plateformes d'accompagnement existantes, basées sur le RGPD, pourraient également être utilisées pour fournir des éclaircissements. En résumé, la concision du texte le rend accessible et compréhensible, mais cette simplicité conduit à des lacunes d'information. Bien qu'il puisse être complété par des lignes directrices et des plateformes d'accompagnement, il n'offre pas une protection renforcée des données ni une meilleure clarté dans leur traitement.
La structure du projet de règlement en permet une consultation efficace et compréhensible. Les différentes sections permettent de bien identifier les obligations quant à la politique de confidentialité et les avis de modification. De plus, la longueur du projet de règlement en facilite la compréhension. Toutefois, afin de s'assurer de cette compréhension et d'éviter des différences d'interprétation, il pourrait être pertinent d'ajouter une section dédiée à certaines définitions. La Loi sur l'accès n'a pas de telle section. En effet, la définition de « renseignement personnel » se trouve à l'article 54 de cette loi et la définition de « renseignement personnel sensible » se trouve à son article 59. Les définitions ne sont donc pas facilement trouvables et cela peut impacter la compréhension de la loi. Ainsi, ajouter dans le projet de règlement certaines définitions permettrait de pallier l'absence d'une telle section dans la loi et d'assurer une meilleure compréhension du règlement. De plus, il pourrait être pertinent d'ajouter davantage de références à la Loi sur l'accès dans le projet de règlement. Par exemple, l'article 5 du projet réfère à l'article 8.1 de la loi pour préciser ce qu'est le comité mentionné. Le même procédé pourrait être fait pour l'article 2(8) du projet de règlement, afin de référer à l'article 8 de la loi, ce qui permettrait de mieux cibler le concept de « responsable de la protection des renseignements personnels ».	Le projet de règlement est court, ce qui en facilite la consultation. Par contre, l'utilisation de termes généraux et peu précis peut entraîner des variations dans son interprétation. L'application du règlement par les organismes qui souhaitent s'y conformer s'en trouvera assurément affectée. C'est pourquoi j'accorde la note de 3,5/5 en ce qui concerne le format du projet de règlement. Après tout, celui-ci vise à déterminer le contenu et les modalités de la politique de confidentialité et des avis de modifications à publier par les organismes publics et devrait donc être rédigé sans équivoque. Par exemple, l'article 2(11) demeure vague à propos de la description des mesures prises pour assurer la confidentialité et la sécurité des renseignements personnels. Il serait utile d'être plus précis et d'exiger la mise en place de mesures contre la perte ou le vol, ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Il serait également profitable de spécifier que ces mesures doivent être physiques, administratives et techniques, et adaptées au degré de sensibilité des renseignements (voir LPRPDE, Annexe 1, principe 4.7). Il serait donc à propos de définir également certains termes, tels que « renseignement personnel », ainsi que « renseignement personnel sensible », comme c'est le cas dans la *Loi sur le secteur privé*.
Je pense que le projet de règlement est assez clair. Je tire cette conclusion du fait que le texte	Le projet de règlement est rédigé en des termes compréhensibles et est divisé en sections bien

est court, concis et précis. Il ne contient que 8 articles, ce qui rend sa lecture plus agréable. Aussi, mis à part l'article 2 qui est long, on peut argumenter que les autres articles sont relativement courts et le vocabulaire utilisé est accessible à tous. De mon point de vue, ce ne sont pas des termes qui sont trop juridiquement complexes. Au lieu d'être de longs paragraphes interminables, on retrouve des énumérations sous forme de puce ce qui facilite également la lecture. Peut-être que le projet de règlement serait encore plus compréhensible pour le public en général s'il était accompagné d'exemples. Ces exemples pourraient se trouver dans un document à part. Ce serait un outil de vulgarisation. Ce n'est pas fréquent, mais je ne vois pas pourquoi ce ne serait pas possible. Évidemment, le projet de règlement peut être difficile à consulter pour l'utilisateur moyen, puisqu'il se trouve dans un lourd document de plus d'une centaine de pages. Or, avec une simple recherche internet, on trouve plusieurs documents et sites web qui traite du projet de règlement. En effet, le projet de loi 64 (alias la Loi 25) a fait l'objet de plusieurs publications. Bref, c'est relativement facile d'être au courant des principes qui émaneront du projet de loi, mais c'est plus difficile d'y avoir accès concrètement.	identifiées qui viennent grandement en faciliter sa lecture et sa consultation. Aussi, le fait que le texte soit court confère au projet de règlement un caractère de synthèse qui intéressera plus de lecteurs, ce qui lui assure une plus grande portée. Cependant, il manque énormément de définitions à l'article 1 (comme les définitions de politique de confidentialité, de renseignements personnels et de moyen technologique) ainsi que de références aux principes de la loi habilitante (la Loi sur l'accès) qui auraient été importantes dans un objectif de clarification et ainsi pour éviter toute ambiguïté quant à l'interprétation du règlement. Effectivement, il s'agit d'un règlement qui possède une plus grande susceptibilité de consultation par les citoyens en raison de sa portée et du caractère sensible de l'objet qu'il traite aux yeux de la population, soit le contenu de politiques de confidentialité des organismes publics visant ultimement à une meilleure protection des renseignements personnels des citoyens concernés. Ainsi, ce règlement devrait être rédigé de sorte à faciliter la compréhension du plus grand nombre et à considérer que ce ne serait pas tout le monde qui aurait d'emblée pris connaissance des dispositions de la loi habilitante (Loi sur l'accès).
Le format du projet de Règlement est en soi facile à consulter. Toutefois, il n'est selon moi pas adapté et suffisamment clair en gardant les objectifs de celui-ci en tête. Un des aspects les plus pertinents à discuter en mon opinion est le manque de précision quant aux différents termes employés dans la rédaction du projet de Règlement. Prenons en exemple l'art. 2(11), qui mentionne que l'organisme public devra inscrire « une brève description des mesures prises pour assurer la confidentialité et la sécurité des renseignements personnels ». Selon moi, l'utilisation des mots « brève description » est très vague et ne permet pas de rejoindre l'intention du législateur d'assurer une uniformisation du contenu présent dans les politiques de confidentialité. Bien qu'il s'agisse d'un terme simple et clair, il n'est pas pour autant précis et laisse place à interprétation par chaque organisme public. Un autre exemple qui me semble pertinent de mentionner est celui de l'art. 3 du Règlement. Il est indiqué qu'une politique de confidentialité peut être commune à plusieurs organismes publics dans la mesure où ils recueillent des renseignements personnels communs. Cette formulation manque un grand manque de précision quant aux conditions devant être remplies pour permettre une telle utilisation commune. S'agit-il seulement de 3 informations qui permettent une telle utilisation ou faut-il	Le règlement est court, donc on lui accorde le mérite d'aller droit au but. Il répond aussi à certaines questions soulevées par l'article 63.4, notamment en détaillant le contenu de la politique et de l'avis de modification. En revanche, certaines dispositions sont nébuleuses ou incomplètes. Notamment l'article 2 (détaillant le contenu de la politique) est incomplet et les articles 3 (décrivant la politique commune) et 7 (qui impose l'obligation d'informer l'individu) nécessitent certaines clarifications. Afin de dissiper ces incertitudes, il serait loisible à la CAI d'élaborer des lignes directrices (article 123 (9) *Loi sur l'accès*) pour clarifier l'approche préconisée et faciliter la conformité au règlement en conséquence (voir celles du WP29 pour le RGPD). À l'instar des Lignes directrices sur le consentement (et du WP29), des exemples d'application pourraient faciliter la conformité aux exigences règlementaires en clarifiant les attentes de la CAI. De même, l'usage de lignes directrices peut offrir une flexibilité plus intéressante, permettant de mettre l'emphase sur des exemples innovants tirés des meilleures pratiques de l'industrie. Par exemple, les lignes directrices pourraient citer des exemples de politiques de confidentialité présentées par un vidéo ou un jeu, deux outils qui s'avèrent plus stimulants pour l'usager. Les lignes directrices pourraient aussi présenter l'exemple du format

plutôt que l'intégralité des renseignements personnels soit commune à chacun des organismes souhaitant faire une politique commune ?	question-réponse pour faciliter la compréhension d'une politique de confidentialité en faisant usage d'une présentation adaptée à la perspective du lecteur. Ces exemples démontrent bien qu'une ligne directrice serait un complément adéquat (ou même une alternative) permettant de clarifier certains éléments.
De prime abord, on peut noter que le corps du projet de règlement semble clair. La division en sections permet d'en faciliter la consultation, ce qui semble adapté pour les organismes publics qui devront rédiger leur politique. Si le texte nous apparaît clair, ce sont les conséquences qui peuvent découler de certaines dispositions qui nous semblent plus incertaines, comme cela a été remarqué précédemment. Cependant, à la lecture de l'introduction, plusieurs éléments questionnent le lecteur. Tout d'abord, comme souligné précédemment, la question de la présence du terme PME se pose. On ne comprend pas vraiment pourquoi le législateur se sent obligé de préciser que les PME ne sont pas concernées par le projet de règlement. Ce point mériterait d'être clarifié car pour l'heure, plusieurs hypothèses peuvent être évoquées. Les organismes publics pourraient ressentir un malaise lors de l'élaboration de la politique de confidentialité en pensant qu'ils passent peut-être à côté de l'esprit du présent règlement. Par ailleurs, on notera également la redondance concernant l'affirmation selon laquelle les ordres professionnels sont concernés par le projet de règlement. Le lecteur peut s'interroger à la fois sur la nécessité de cette précision et aussi sur le fait qu'elle apparaît à deux reprises. Cette attention toute particulière aux ordres professionnels mériterait également d'être clarifiée selon nous. Enfin, il nous semble que la neutralité technologique ne soit pas prévue par le règlement, ce qui est non conforme à la Loi dont il découle.	Je suis d'avis que le format du projet de règlement est facile à consulter, en effet les différentes sections permettent de simplifier la navigation au sein du projet de règlement. De plus, les différents articles du règlement sont divisés de manière logique. Ce format est adapté afin de faciliter son adoption par les organismes publics. Le texte est rédigé avec des termes simples, toutefois malgré l'utilisation de termes simples, certains passages étaient plus complexes à la lecture, à titre d'exemple, le passage suivant, « une politique de confidentialité ne peut être modifiée avant l'expiration d'un délai de 15 jours à compter de la date de publication d'un avis de modification de cette politique », m'a semblé ardue à bien comprendre et interpréter. De plus, le terme « recueillir » est utilisé en alternance avec le terme « collecter » dans le projet de règlement. Toutefois, cette alternance, à mon avis, complexifie la compréhension du texte. Un exemple, dans ce projet de règlement illustrant cette situation, est le fait qu'à l'article 2, alinéa 1, on indique « nom de l'organisme public qui recueille les renseignements personnels », tandis qu'à l'article 7, on indique « lors de la collecte de renseignements personnels par un moyen technologique ». En ce sens, à mes yeux, il sera plus facile d'utiliser un seul terme pour faciliter l'application du règlement, et si ces termes ne sont pas substituants, il serait pertinent de le soulever.

2. QUESTIONS SPÉCIFIQUES

2.1 Article 1 : Que pensez-vous du champ d'application du projet de règlement ? Est-ce que tous les organismes publics ainsi que le secteur privé devraient y être assujettis ?

À mon avis, le champ d'application du projet de règlement devrait être élargi. Premièrement, le projet est édicté en conformité avec la disposition 63.4 de la LAI, qui s'applique uniquement aux organismes publics ciblés. Ainsi, le projet de règlement n'a aucune conséquence pour entreprises du secteur privé, car ces dernières ne sont pas visées. Dans la *Loi sur la*	Je suis d'accord avec le champ d'application du projet de règlement, plus spécifiquement, que le projet de règlement vise uniquement les organismes publics. Premièrement, le secteur privé et le secteur public sont assujettis à des lois distinctes sur la protection des renseignements personnels. En adoptant la Loi sur l'accès et la Loi sur le secteur privé, le législateur a créé deux

protection des renseignements personnels dans le secteur privé (ci-après « LP »), il n'est pas prévu que le contenu et les modalités de la politique de confidentialité et de l'avis puissent être déterminés par règlement. Ainsi, les obligations concernant la politique de confidentialité seront différentes pour les deux secteurs. Les organismes publics seront assujettis à des obligations beaucoup plus sévères, ou du moins beaucoup plus détaillées que les entreprises privées. Deuxièmement, ce projet de règlement ne s'applique qu'à l'organisme qui récolte les renseignements personnels par moyen technologique. En effet, un régime distinct et moins précis est applicable lorsque les renseignements sont récoltés par un autre moyen, notamment par téléphone. En effet, il s'agit de l'article 65 de la LAI qui s'appliquera dans ce cas-ci. À mon avis, le projet de règlement devrait être applicable aux organismes des deux secteurs, et ce peu importe le moyen utilisé pour la récolte. En effet, les objectifs de transparence et d'harmonisation poursuivis par ce dernier sont importants en matière de protection des renseignements personnels. À titre d'exemple, le RGPD est, quant à lui, applicable à tout organisme qui collecte et manipule des données à caractère personnel. Toutefois une telle modification de l'article premier demanderait des ajustements significatifs au niveau des lois habilitantes également. Bref, un champ d'application plus étendu pourrait maximiser les impacts positifs en matière de transparence.	régimes distincts en matière de protection des renseignements personnels. Fusionner les deux régimes distincts uniquement pour les fins du projet de règlement susciterait de la confusion. Deuxièmement, tout règlement doit découler d'une loi habilitante qui confère au gouvernement le pouvoir d'adopter un règlement. Le présent projet de règlement a été adopté en vertu de la Loi sur l'accès et non en vertu du Loi sur le secteur privé. La Loi sur le secteur privé ne confère pas au gouvernement le pouvoir d'élaborer un règlement pour déterminer le contenu et les modalités d'une politique de confidentialité alors qu'en vertu de son article 63.4, lequel entrera en vigueur le 22 septembre 2023, et son article 155, la Loi sur l'accès confère au gouvernement le pouvoir d'en élaborer un. De plus, je crois qu'il est approprié que le projet de règlement s'applique à tous les organismes publics pour assurer une bonne uniformité. La politique de confidentialité a pour but de faire comprendre aux individus leurs droits et la manière dont les renseignements personnels sont recueillis et utilisés. En assujettissant tous les organismes publics au présent règlement, tous les individus auront accès aux mêmes informations lors d'une collecte de renseignements personnels.
Compte tenu que le projet de règlement a pour but la modification de la loi sur l'accès, seuls les organismes publics y sont assujettis. Toutefois, une mesure similaire est également prévue pour les renseignements personnels détenus par un organisme privé (en respect avec la définition d'entreprise à l'article 1525 du Code Civil du Québec) qui les obligent également à créer une politique de confidentialité pour la collecte de renseignements personnels. Par souci de concision et d'efficacité, le champ d'application de ce règlement aurait pu être autant au niveau du secteur privé que public, tel que dans le RGPD, compte tenu de la grande similarité entre les deux lois. Des directives claires et précises concernant les obligations pour la création de politiques de confidentialité auraient pu être applicables aux organismes privés et publics. De plus, comme le CAI est le gardien de la mise en application de ses deux lois, l'application au niveau public et privé aurait été plus simple et cela aurait également facilité la surveillance de l'application de la mesure. De plus, autant la loi publique que privée se doivent de suivre les lignes directrices du CAI concernant le consentement. Avoir un cadre	L'article 1 réfère aux organismes publics visés à l'article 3 de la *Loi sur l'accès*, mais précise également le statut des ordres professionnels, dont le statut juridique est parfois nébuleux. Il aurait été utile d'ajouter d'autres organismes à cette liste, ainsi que les organismes parapublics. En effet, selon le Global Right to Information Rating, un des principaux problèmes de la loi québécoise avant la Loi 25 était son champ d'application trop restreint (Rétablir l'équilibre, p.11). « Si le champ d'application de cette loi n'est pas suffisamment large, des renseignements d'intérêt public risquent de se trouver hors de sa portée et, par conséquent, d'être exclus des obligations de transparence souhaitées lors de l'adoption de la Loi sur l'accès. » (Rétablir l'équilibre, p.12). Par contre, le champ d'application de ce règlement ne saurait inclure des entreprises du secteur privé, puisqu'il est édicté en vertu de l'article 63.4 de la *Loi sur l'accès*, loi s'appliquant seulement aux organismes publics. Si le Québec et le reste du Canada traitent distinctement le public et le privé dans l'encadrement législatif de la protection des renseignements personnels, il en est autrement

unique concernant la confidentialité des renseignements personnels aurait également prévu des liens économiques plus simples pour les collaborations entre le système public et privé. Également, une harmonie dans les pratiques de politiques de confidentialité favoriserait des collaborations entre le privé et le public en évitant de dédoubler les obligations légales selon le secteur de pratique. Par exemple, dans le contexte présent de collaboration dans les services de soins de santé entre le public et le privé, une politique harmonisée avec les mêmes exigences permettrait une transition plus simple.	ailleurs dans le monde (voir RGPD). Aussi, le champ d'application devrait préciser que l'ensemble du cycle de vie de l'information est visé par ce règlement, à l'instar de la règlementation européenne et de la *Loi sur la protection des renseignements personnels*. Le premier alinéa de l'article 1 du projet de règlement pourrait se lire ainsi : « Le présent règlement s'applique à tout organisme public ou parapublic qui traite des renseignements personnels dans l'exercice de ses fonctions ».
À mon avis, le champ d'application du projet de règlement semble illogique. Ce règlement découle de la Loi 25 et, plus particulièrement, sert à apporter certaines précisions quant à son application lorsqu'elle entrera en vigueur en septembre 2023 (deuxième vague de changements). La Loi 25 est une loi modificatrice qui apporte des changements importants, tant pour le secteur privé que pour le secteur public. Ainsi, il me semble logique que le règlement s'adresserait aux deux secteurs, comme la Loi 25, et non seulement au secteur privé. Je m'explique : ce règlement a été rédigé en raison de l'article 63.4 de la Loi sur l'accès (introduit par la Loi 25) qui impose aux organismes publics recueillant des renseignements personnels de tenir une politique de confidentialité. Toutefois, l'article 8.2 de la même loi exige aussi des entreprises de rédiger une telle politique, dans le cas qu'elles recueillent des renseignements personnels. Ainsi, pourquoi ériger un règlement qui permet de ne préciser la mise que pour les organismes publics alors que les entreprises privées ont la même obligation ? On mentionne dans le préambule du projet de règlement qu'il permettra « d'harmoniser le contenu des politiques de confidentialité des organismes publics », mais pourquoi ne voudrait-on pas la même chose de la part du secteur privé ? Il me semble évident que cela rendrait les choses d'autant plus faciles et plus claires pour les utilisateurs et les consommateurs, considérant en outre que les politiques de confidentialité des entreprises sont extrêmement hétérogènes entre elles. Ainsi, je crois qu'il devrait être ajouté, à la fin de l'article 1 du Règlement, ceci : « Il s'applique finalement aux entreprises, au sens de l'article 1525 du Code civil du Québec. »	Je crois que le fait de restreindre le champ d'application de ce projet de règlement au secteur public est justifié. Bien que le *Règlement général sur la protection des données* (ci-après « RGDP ») ait choisi de ne pas séparer les deux secteurs, je suis d'avis que les secteurs privés et publics doivent faire l'objet de considération distincte et ne devraient pas nécessairement être soumis aux mêmes obligations, notamment en matière de transparence. En effet, le traitement des données est généralement différent, car la finalité des secteurs est différente. En vertu de l'article 1525 al.3 C.c.Q., l'objectif premier d'une entreprise est de mener des activités commerciales et de réaliser du profit, alors que les organismes publics visent généralement l'intérêt public (Journal des débats, 2020). Ainsi, les usagers ont généralement des attentes plus élevées envers le secteur public quant aux partages des données avec des tiers. Par ailleurs, les organismes publics traitent souvent des données plus sensibles comme le numéro d'assurance sociale, la date de naissance, l'état de santé, les antécédents médicaux ou encore des renseignements financiers. De plus, le consentement de l'utilisateur dans certaines situations n'est pas toujours libre. Par exemple, un individu est tenu de fournir des renseignements financiers pour sa déclaration d'impôt. En revanche, dans le secteur privé, le principe du libre-marché facilite généralement le choix de ne pas consentir à partager ces renseignements. En outre, les sanctions devraient varier en fonction des secteurs. Dans le cas du secteur privé, il est plus justifiable d'imposer des sanctions pénales plus élevées, puisqu'au public, ces amendes seraient finalement supportées par les contribuables. Compte tenu de ces considérations, le fait d'appliquer le projet de règlement aux deux secteurs engendrait probablement plus de confusion que de clarté. Cette séparation permet

	donc d'offrir une meilleure protection des données sensibles.
L'article 1 démontre que le projet de règlement s'applique à certains organismes publics et aux ordres professionnels. Ce règlement est donc spécifique au secteur public, et prennent en compte, entre autres, le gouvernement, les établissements de santé ou de services sociaux, les organismes gouvernementaux, etc. Les organismes publics doivent avoir la confiance des citoyens pour pouvoir fonctionner efficacement. Ceux-ci conservent aussi plusieurs renseignements personnels. Le public devrait donc être capable de s'informer facilement sur la conservation et l'utilisation de leurs données par les organismes publics. Par exemple, les services de santé ont accès à des renseignements personnels sensibles, et les personnes qui accèdent à ses services sont en droit de s'attendre à ce que la confidentialité de leurs informations soit règlementée. De plus, les ordres professionnels ont pour mission principale d'assurer la protection du public, selon l'Office des professions du Québec. Les ordres professionnels peuvent aussi communiquer des renseignements personnels, en vertu de l'article 108.10 du *Code des professions*. Il est donc particulièrement important que des règles spécifiques s'appliquent aux ordres professionnels pour qu'ils puissent communiquer les informations nécessaires sans brimer leur mission principale. L'idée de règlementer les politiques de confidentialité des ordres professionnels est donc particulièrement importante, pour permettre d'assurer une protection plus complète du public et de garder la confiance de celui-ci. Ainsi, je considère qu'il est pertinent que le règlement s'applique spécifiquement aux organismes publics et aux ordres professionnels, car ceux-ci sont placés dans une situation particulière avec le public, qui n'est pas la même que le secteur privé. Il est donc normal que les attentes du public ne soient pas les mêmes. Cette relation de confiance doit donc s'inscrire dans la législation québécoise, et je considère que le règlement est un pas dans cette direction.	En ce qui a trait au champ d'application du règlement, je crois que le secteur privé devrait y être assujetti mais seulement en partie. Tout d'abord, je comprends que, par l'exclusion du secteur privé du règlement, une certaine discrétion a voulu être accordée aux entreprises en ce qui a trait à la mise en place de la politique de confidentialité, particulièrement pour les plus petites entreprises. Toutefois, un certain encadrement quant au contenu de la politique peut s'avérer nécessaire afin d'assurer une uniformité aux usagers et consommateurs du secteur privé. Bien que, dans le préambule du projet de règlement, il est mentionné que « le projet n'a pas de conséquence sur les entreprises, en particulier les PME », je pense qu'il serait important que l'article 2 s'applique au secteur privé afin que l'objectif initial du projet de règlement d'harmonisation du contenu des politiques de confidentialité soit atteint avec plus d'efficacité. Ainsi, le secteur privé, tout comme les organismes publics et les ordres professionnels, pourrait bénéficier de directives dans la rédaction de leur politique de confidentialité. En ce qui concerne les autres dispositions du projet de règlement, je considère qu'elles sont moins pertinentes ou non applicables au secteur privé. Par exemple, lorsqu'il est question de l'article sur les politiques communes, un tel principe peut difficilement s'appliquer à des entreprises privées en raison de leur nature. De plus, pour ce qui est de l'article 5 concernant la consultation par le CAI préalablement à la publication de la politique, le fait d'étendre la portée de cet article au secteur privé aurait pour effet de donner un énorme volume de travail au CAI, ce qui se traduirait par de longs délais avant de pouvoir publier ladite politique. Ainsi, je propose que le projet de règlement s'applique au secteur privé mais seulement en partie.
L'article 1 de ce projet joue un rôle fondamental en établissant le champs d'application de ladite loi. Cependant contrairement à la loi sur le secteur privé, il ne fournit pas de définition la notion de renseignements personnels. Pour le secteur privé, les renseignements personnels englobent tout ce qui est « recueilli, détenu, utilisé ou communiqué ». Cette définition diffère	Le champ d'application du projet de règlement réfère « à tout organisme public visé à l'article 3 de la Loi », ainsi qu'aux ordres professionnels. Toutefois, l'article 63.4 de la Loi sur l'accès mentionne que la publication d'une politique de confidentialité s'adresse à un organisme public qui recueille « par un moyen technologique » des renseignements personnels. De plus, le titre du

de celle du RGPD, qui intègre le terme de « traitement », reflétant potentiellement une perspective plus large. Cette absence créé un manquement à l'objectif principale du projet qui est la transparence. En outre, l'article 1 trace les contours du domaine d'application de la loi en spécifiant qu'elle concerne exclusivement le secteur public. Cette distinction est notable. Contrairement au RGPD qui s'applique tant au secteur public qu'au secteur privé, la loi crée une démarcation nette entre ces domaines. Cette séparation peut engendrer une certaine complexité et confusion, surtout au Canada où déjà une complexité similaire entre les lois fédérales et provinciales existe. On peut alors s'interroger sur la nécessité d'une multiplication de réglementation, d'autant plus que leur principe se rejoignent. En effet, la dualité entre les juridictions fédérales et provinciales au Canada peut rendre la situation encore plus délicate, car cela signifie qu'il existe déjà une superposition de lois et de réglementations. L'ajout d'une distinction entre les secteurs public et privé pourrait entraîner davantage de complications pour les organisations et les individus qui doivent naviguer entre différents niveaux de conformité. En somme, bien que l'article 1 de la loi établisse avec clarté le champ d'application, la distinction entre secteur public et privé pourrait potentiellement complexifier davantage le paysage législatif canadien, en particulier compte tenu des diverses juridictions et des interactions avec le RGPD. Une approche harmonisée pourrait faciliter la compréhension et la mise en œuvre de la réglementation.	projet de règlement fait référence aux organismes publics recueillant des renseignements personnels « par un moyen technologique ». Ainsi, il serait pertinent, par principe de cohérence, de préciser dans le champ d'application (art.1) cette particularité technologique. Quant à l'exclusion du secteur privé, il serait pertinent de reconsidérer la possibilité d'assujettir les entreprises. En effet, selon les travaux parlementaires, l'objectif d'un tel règlement est la standardisation des politiques de confidentialité. Ainsi, pourquoi ne pas standardiser l'ensemble des secteurs ? La combinaison public/privé n'alourdirait pas le règlement de manière à en impacter sa compréhension. De plus, l'introduction au projet de règlement indique que « ce projet de règlement n'a pas de conséquence sur les entreprises, en particulier les PME ». Il y a donc une volonté d'exclure les PME. On pourrait donc inclure les entreprises dans le champ d'application tout en excluant les PME. Cependant, l'article 8.2 de la Loi sur le secteur privé ne fait pas mention d'une possibilité de règlementer, contrairement à l'article 63.4 al.2 de la Loi sur l'accès. On peut donc se questionner quant à l'effet pratique d'une telle absence de règlement pour le secteur privé. Sans règlement, les entreprises n'auront pas d'autres choix que d'aller voir ce qui se fait au public pour rédiger une politique adéquate. S'il est impossible d'inclure le secteur privé au règlement, la rédaction de lignes directrices pourrait être une solution envisageable (art. 123(9) Loi sur l'accès).
Le champ d'application du projet de règlement est trop restreint et devrait s'appliquer aux organismes publics visés par la Loi sur l'accès ainsi qu'au secteur privé. Le projet de règlement poursuit deux objectifs généraux, soit l'harmonisation du contenu des politiques de confidentialité des organismes publics qui seront rendues disponibles lors d'une collecte de renseignements personnels par un moyen technologique ainsi que, de ce fait, l'information des citoyens quant à leurs droits ainsi qu'au recueil et à l'utilisation de leurs renseignements personnels. La Loi sur l'accès ainsi que la Loi sur le secteur privé ont l'objectif commun de protection des renseignements personnels et devraient ainsi recevoir les mêmes traitements et interprétations. En revanche, la restriction du champ d'application du projet de règlement seulement aux organismes publics visés par la Loi sur l'accès limite considérablement l'harmonisation globale du contenu des politiques de confidentialité par l'instauration d'un traitement différent entre les deux lois. Aussi,	À mon avis, le projet de règlement ne devrait pas se limiter seulement au secteur public. La Loi sur l'accès et la Loi sur le secteur privé, sans dire qu'elles sont identiques, sont des lois jumelles. Elles présentent des normes qui sont très similaires sur le plan pratique. Cela milite en faveur d'un projet de règlement qui serait applicable aux deux secteurs. Cependant, à ce sujet, il importe de soulever que le nouvel article 63.4 applicable au secteur public, prévoit que : « Un règlement du gouvernement peut déterminer le contenu et les modalités de cette politique et de cet avis ». Or, l'article 8.2 applicable au secteur privé n'a pas cette mention. Il serait intéressant de rajouter un deuxième alinéa à cet article afin de prévoir un pouvoir similaire. On pourrait par exemple s'inspirer de la mention à l'alinéa 4 de l'article 3.5 de la Loi sur le secteur privé. Si tel était le cas, je pense que rien ne justifierait de ne pas assujettir le privé au même titre que les organismes publics. À ce sujet, il faudrait prendre en considération le fait

l'objectif de transparence poursuivi par le projet de règlement devrait être constant dans toutes les politiques de confidentialité car les enjeux individuels qui en découlent sont universels. Par ailleurs, il serait cohérent que le règlement ait compétence sur les politiques de confidentialité du secteur privé puisque l'article 8.2 de la Loi sur le secteur privé est rédigé sensiblement de la même manière que l'article 63.4 de la Loi sur l'accès. Toutefois, il n'en est pas de même des organismes n'étant assujettis à aucune des deux lois qui devront se rabattre aux règles de droit commun. Ainsi, il serait utile d'ajouter au premier article du projet de règlement que ce dernier s'applique aussi au secteur privé. Étant donné que la Loi sur le secteur privé inclut les ordres professionnels en son article 1 alinéa 3, l'article 1 alinéa 2 du projet de règlement devient obsolète et peut être supprimé.	que ce ne sont pas tous les entreprises du secteur privé qui détiennent les mêmes ressources et qui pourront mettre en œuvre le règlement de la même façon. Il faudrait peut-être que le règlement établisse des distinctions entre les PME et les grandes entreprises qui sont financièrement bien établies. Les délais pourraient différer et de plus amples ressources pourraient être octroyés aux PME. Voici une nouvelle version du premier alinéa de l'article 1 : « Le présent règlement s'applique à tout organisme public visé à l'article 3 de la Loi sur l'accès […] ainsi qu'à toutes les organisations qui exploitent une entreprise au sens de l'article 1525 al. 3 du Code civil du Québec (chapitre CCQ-1991) ».
À la lecture de l'article, le champ d'application semble bien défini. Il en ressort clairement que ce texte s'applique aux organismes publics québécois ainsi qu'aux ordres professionnels. En revanche, les entreprises auraient aussi intérêt à y être assujettis, car, selon le nouvel article 3.2 *Loi sur le secteur privé*, ceux-ci sont soumis à une obligation équivalente. Au lieu de détailler le contenu de la politique à même cet article, le législateur devrait plutôt préciser les obligations des entreprises par l'entremise du même règlement. Ainsi, l'objectif d'harmonisation pour l'individu est mieux servi en soumettant les entreprises (art. 1525 al. 3 CcQ) aux exigences du règlement. Un champ d'application complet emporte un standard à travers le Québec qui est particulièrement intéressant pour le consommateur moyen plutôt pressé confronté à plusieurs politiques. Au final, c'est surtout la protection de ses renseignements personnels qui compte pour ce dernier, sans égard à la distinction entre un organisme public (Hydro-Québec) et une entreprise privée (Vidéotron). Une application plus complète assure donc une réelle harmonisation du contenu des politiques présentées à l'individu afin d'obtenir les informations nécessaires au consentement éclairé. *Le règlement s'applique également aux entreprises et aux partis politiques, député indépendant ou candidat indépendant visé par l'article 1 de la Loi sur le secteur privé*. Une nuance doit être apportée. La pertinence d'une politique de confidentialité se limite aux entreprises qui traitent un certain volume de renseignements personnels ou de renseignements sensibles. Pour cerner la distinction, il est possible d'appliquer, par analogie, les critères de 37(1) *RGPD* qui déterminent quelles organisations traitent	Le projet de règlement s'applique uniquement aux organismes publics, qui sont définis à l'article 3 de la Loi sur l'accès, et aux ordres professionnels. Toutefois, il s'avère pertinent de se questionner sur la possibilité de considérer une réglementation unique, au Québec, s'appliquant au secteur privé et au secteur public en ce qui attrait aux politiques de confidentialité. En estimant que ce projet de règlement tend à vouloir, tel que mentionné dans le document de discussion, « harmoniser le contenu des politiques de confidentialité » pour les citoyens, ne serait-il pas favorable de soumettre les entreprises, tel que spécifié à l'article 1525, alinéa 3, du Code civil du Québec, ou du moins certaines de ces entreprises, aux mêmes exigences que les organismes publics. Il ne demeure pas réaliste ou nécessaire de soumettre toutes ces entreprises, particulièrement des petites ou moyennes entreprises traitant une quantité minimale de données personnelles, au niveau d'exigence, établis par ce projet de règlement. Toutefois, certaines entreprises collectent un nombre considérable de renseignements personnels, et parfois même de données sensibles, par un moyen technologique. Ainsi, ne serait-il pas plus pertinent de nuancer l'application du règlement en fonction de la quantité de renseignements personnels ou de la sensibilité de ces mêmes renseignements ? À mes yeux, la mise en oeuvre de ce nouveau champ d'application serait favorable. Ce nouveau champ d'application impliquerait une modification de l'article 1 du projet de règlement, qui devrait dorénavant appliquer le présent règlement aux entreprises, au sens de l'article 1 de la Loi sur la protection des renseignements personnels dans le secteur privé (*Loi dans le secteur privé*) qui

suffisamment de données pour devoir nommer un délégué à la protection des données. En limitant le champ d'application aux entreprises traitant un certain volume de données (balise inspirée de 37(1) *RGPD*), cela exempte les PME d'une obligation qui n'est pas proportionnelle à leurs activités.	traite d'une quantité ou d'un niveau de sensibilité de données qui se devrait d'être déterminé par des experts.
Un règlement est un acte normatif édicté en vertu d'une Loi. Le présent projet de règlement est édicté en vertu de l'article 63.4 de la Loi sur l'accès. Cette Loi concerne les organismes publics, dont les ordres professionnels. Le règlement pourrait donc avoir pour champ d'action les organismes publics, dont les ordres professionnels. La Loi exclut certains registres, le règlement ne s'appliquerait pas pour ces derniers. Pourtant, l'article 1 du projet indique que les organismes publics visés par le règlement sont ceux prévus à l'article 3 de la Loi sur l'accès et précise que les ordres professionnels sont aussi concernés, alors que ces derniers sont cités à l'article 1.1 de la Loi sur l'accès. Ceci porte à confusion. Par ailleurs, il n'y a aucune raison juridique pour que le règlement s'applique au secteur privé. C'est la Loi sur le secteur privé qui devrait permettre de règlementer sur la question des politiques de confidentialité, mais elle ne le fait pas. Ainsi, pour le secteur privé, seul des actes para-réglementaires (lignes directrices, guides…) pourraient venir préciser le contenu d'une politique de confidentialité. La critique énoncée plus haut sur la précision que les entreprises et particulièrement les PME ne seront pas touchées par ce projet de règlement, peut être réitérée, on ne comprend pas bien la nécessité de ce commentaire. L'article pourrait être rédigé comme suit : « Le présent règlement s'applique à tout organisme public visé par les articles 1, 1.1 et 3 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). » Nous pensons qu'il est dommage que le secteur privé ne puisse être réglementé de la même manière que le secteur public, un défaut d'harmonisation s'annonce, ce qui fera sans doute naître de nombreux enjeux futurs lors de la collaboration intersectorielle public-privé.	Selon moi, nous gagnerions à consolider les secteurs privés et publics. Cela permettrait d'éviter, comme nous le voyons présentement, des incohérences entre les deux secteurs. Consolider les deux secteurs permettrait d'éviter des discordances en s'assurant d'avoir une uniformité globale et d'éviter d'avoir un secteur moins bien encadré permettant ainsi d'atteindre les buts énoncés par le législateur, soit d'uniformiser et de rendre l'information accessible. La *Loi sur l'accès* et la *Loi sur le secteur privé* sont des lois « jumelles » (en majorité) qui nécessitent d'avoir des règlements concernant les politiques de confidentialité qui sont similaires, voire identiques. Le contraire vient créer des inégalités dans le traitement des renseignements personnels, chose qui est absurde puisqu'il s'agit, dans les deux cas, de renseignements personnels identiques qui doivent être protégés de la même manière. Je crois également que tous les organismes publics devraient être inclus sous ce règlement pour les mêmes raisons exprimées ci-dessus. Cette uniformité doit être atteinte, et ce dans tous les secteurs pour atteindre un résultat permettant de bien répondre aux objectifs du législateur. Dans le cas contraire, il s'agit selon moi d'une tentative qui n'est pas suffisante et qui créer d'autres lacunes.

2.2 Article 2 : Que pensez-vous du contenu que devrait contenir une politique de confidentialité ? Est-ce trop ou pas assez détaillé ?

La politique de confidentialité telle qu'inscrite dans le projet de règlement respecte en partie les exigences de politique de confidentialité décrites par les orientations du RGPD et le commissariat à la protection de la vie privée du Canada, mais a de grands manquements. Par exemple, le délai de conservation et les conditions de suppression ne sont pas inscrits dans le projet de règlement. D'abord, concernant le délai de conservation et les conditions de suppression, la Loi 25 pour le secteur privé explique le devoir de définition du délai de conservation des renseignements selon la nature de ces derniers. Aucune mention n'est faite dans le projet de règlement. Il serait donc important de définir le délai de conservation des renseignements selon la nature du renseignement. Par exemple, la conservation des renseignements personnels pour la durée de la finalité. De plus, les lignes directrices du consentement écrites par la CAI indiquent que le consentement doit être temporaire et que la durée doit être déterminée. Lors d'un consentement à long terme, les utilisateurs doivent être rappelés à plusieurs reprises pour confirmer qu'ils ont donné leur consentement. Autrement, le consentement n'est pas libre et éclairé et n'est donc plus valide. Une solution possible serait l'utilisation d'exemples concernant les buts de la collecte de ses renseignements personnels. Il est très important que les utilisateurs comprennent les raisons et l'utilisation de leurs renseignements personnels. De plus, il n'y a présentement aucune mention de l'usage de renseignements personnels pour les mineurs de moins de 14 ans et du besoin de consentement par leurs parents ou tuteurs légaux, tel qu'indiqué dans la loi 25 du secteur privé. De ce fait, le projet de règlement présente une base qui n'est pas assez détaillée pour permettre aux utilisateurs de les informer de l'usage de leurs renseignements personnels.	Je considère que le contenu minimal prévu à l'article 2 du règlement comporte certaines lacunes qui seraient importantes à ajouter dans une politique de confidentialité d'un organisme public. En effet, en ayant décidé de dresser une liste exhaustive des obligations minimales du contenu d'une politique de confidentialité, je considère que cette liste doit être la plus précise possible afin d'éviter que certaines clauses nécessaires à la protection du public soient omises. Premièrement, et le manque le plus frappant à mon égard, est qu'il n'y ait aucune mention du temps que les données personnelles sont conservées. En effet, il ne serait pas raisonnable que les organismes publics conservent à perpétuité les renseignements personnels qu'ils ont recueillis, et ce même si aucun délai n'est pour l'instant prescrit par la loi. On devrait donc trouver dans les clauses obligatoires à la politique de confidentialité expliquant que les données personnelles seront gardées pour un temps raisonnable selon l'utilisation de ses données. Ces données doivent être anonymisées ou détruites après un certain temps et cela devrait aussi être indiqué obligatoirement dans les politiques de confidentialité. Deuxièmement, je considère que le règlement devrait prescrire que la politique de confidentialité contienne minimalement des informations concernant le consentement des mineurs à celle-ci. Cela peut prendre une importance particulière pour les organismes scolaires, qui conservent des informations de mineurs, et qui sont visés par le règlement. Des mineurs peuvent recevoir des services d'organismes publics, et ainsi devoir consentir à la politique de confidentialité. Il serait donc particulièrement important que la politique de confidentialité explique si le consentement des parents est nécessaire, et quels renseignements personnels de personnes mineurs seront conservés.
Pour ce qui est du contenu que devrait contenir une politique de confidentialité, je suis d'avis que l'article 2 est assez bien détaillé et qu'il couvre adéquatement plusieurs éléments essentiels que devrait contenir une politique. Bien que cette disposition soit bien détaillée, j'aimerais proposer certains éléments qui pourraient être ajoutés afin d'être plus précis et d'assurer une meilleure protection des renseignements personnels. Tout	Je m'interroge sur la pertinence et/ou la formulation des paragraphes 11, 12 et 13 de l'article 2 du projet de règlement. En ce qui concerne l'obligation d'inclure une brève description des mesures prises pour assurer la confidentialité et la sécurité des renseignements, je suis d'avis qu'informer les Québécois des mesures de sécurité mises en place pourraient sans doute les rassurer d'une certaine manière,

d'abord, il serait intéressant d'aborder les témoins de connexion (cookies) dans l'article 2 du projet de règlement. En effet, dans le mémoire du 20 juin 2023 par le Ministre responsable de l'Accès à l'information concernant le projet de règlement, il a été mentionné que les cookies pouvaient être un moyen par lesquels les renseignements personnels peuvent être recueillis. En ce sens, il pourrait y avoir un ajout dans les politiques concernant les témoins de connexion, notamment l'information collectée automatiquement, le type d'information collectée et les fins d'utilisation des cookies spécifiquement. Par exemple, à la fin du paragraphe 5, il pourrait être mentionné « […] notamment, par des témoins de connexion, etc. ». Ensuite, je propose également un ajout à cette disposition qui mentionnerait les modalités concernant la conservation et la destruction, le cas échéant, des données personnelles recueillies. À titre d'exemple, le Commissariat à la protection de la vie privée du Canada possède notamment une section attribuée à ce sujet dans sa politique de confidentialité. De plus, une obligation similaire se retrouve à l'article 3.2 de la Loi sur la protection des renseignements personnels dans le secteur privé : « […] doivent notamment prévoir l'encadrement applicable à la conservation et à la destruction de ces renseignements […] ». Ainsi, le projet de règlement pourrait intégrer à son contenu la même obligation que la loi fédérale afin de mieux protéger les renseignements personnels.	mais en dévoilant les mesures de sécurité mises en place cela pourrait aussi entraîner des effets pervers. Ainsi, je suggère que l'obligation soit d'indiquer dans la politique les types de mesures de sécurité prises par l'organisme, soit les mesures matérielles, les mesures administratives et les mesures techniques, sans plus d'approfondissement. De plus, puisque les règles de gouvernance dans lesquels est prévu le processus de traitement des plaintes doit également être publié sur le site internet de l'organisme public en vertu de l'article 63.3 de la Loi sur l'accès, je crois que le paragraphe 12 de l'article 2 du projet de règlement devrait aussi mentionner que l'hyperlien vers les règles de gouvernance, lesquelles prévoient le processus de traitement des plaintes relatives à la protection des renseignements personnels, doit être inclus dans la politique. En plus de fournir le nom et les coordonnées de la personne responsable de la protection des renseignements personnels de l'organisme public, les coordonnées de la personne, de l'organisme concerné ou d'une unité administrative de ce dernier à qui toute relative à cette politique de confidentialité peut être soumise doivent également être fournis dans la politique de confidentialité en vertu de l'article 2(13) du projet de règlement. Je suis d'avis que toute question relative à la politique devrait être soumise au responsable de la protection des renseignements personnels de sorte que le paragraphe 13 n'est pas nécessaire.
Pour maximiser les impacts positifs, le contenu de la politique édicté dans le projet de règlement pourrait être plus détaillé. D'abord, il pourrait être ajouté au contenu minimum des informations sur la durée de conservation des renseignements personnels et sur la fin du cycle de vie du renseignement. Ces deux informations sont d'ailleurs des exigences prévues par le RGPD à l'article 13. De plus, il pourrait y avoir une mention indiquant que l'organisme peut communiquer les renseignements personnels sans le consentement de la personne visée, tel que le recommande la CAI dans les lignes directrices sur le consentement 2023-1 (principe 1.3.1.4). Finalement, il serait bien que la politique comporte des mentions sur le traitement des témoins ou des fonctions d'identification, de localisation et de profilage. Pour le secteur privé, on retrouve une telle exigence (LP, article 8.1). Ensuite, une problématique liée aux politiques de confidentialité est, selon moi, l'accessibilité de l'information. En effet, une politique de confidentialité qui s'étend sur des dizaines de pages et dont la lecture nécessite un temps	L'article 2 énumère quatorze points qui doivent faire l'objet de la politique. À mon avis, c'est beaucoup. Il est admis que la plupart des utilisateurs ne prendront pas le temps de lire les politiques de confidentialité et ils ne le feront pas, à plus forte raison, si elles sont longues et trop détaillées. À mon avis, il faudrait que le contenu essentiel pour l'utilisateur moyen soit présenté de manière accrocheuse et stimulante. La politique ne devrait pas simplement prendre la forme d'un texte continue et monochrome comme la plupart des politiques actuellement en circulation. Le Commissariat à la protection de la vie privée du Canada (ci-après « CPVP ») indique dans ses travaux que les éléments suivants méritent une attention particulière lors de la rédaction d'une politique de confidentialité : personne-ressource, collecte, utilisation, communication, conservation et accès. Il serait intéressant que ces éléments se retrouve en plus grand caractère et en gras, question de rapidement les identifier. Le reste des informations prévues à l'article 2 devront également figurer à la politique, car elles demeurent importantes et sont essentielles pour que le consentement de l'utilisateur soit valide.

significatif à la personne moyenne perdra tout son sens. La LPRPDE (article 4.8.1) prévoit qu'une personne devrait pouvoir obtenir sans effort déraisonnable de l'information au sujet des pratiques d'une organisation. D'ailleurs, le Commissariat encourage l'usage d'un langage simple et clair, d'une structure conviviale, dans un document est aussi court que possible tout en fournissant l'information nécessaire (novembre 2018, lien). Dans ses lignes directrices sur le consentement, il recommande aussi l'accentuation des éléments clés pour que les individus prennent rapidement conscience des éléments qui auront une incidence sur leur décision (août 2021, lien). La CAI y fait également référence dans ses lignes directrices sur le consentement. À l'article 63.4 LAI, on inclut l'obligation d'user d'un langage simple et clair, mais le règlement pourrait préciser d'autres balises quant au format.	Elles pourraient être présentées de façon « standard », c'est-à-dire sous la forme d'un texte continu noir et blanc. Voici une version modifiée de l'article 2 : « Une politique de confidentialité visée à l'article 63.4 de la Loi doit minimalement contenir : 1° à 7 [les paragraphes 1 à 7 devraient contenir les informations énumérées ci-dessus proposées par le CPVP]. Les informations figurant aux paragraphes 1 à 7 doivent être indiqués de façon à attirer l'attention du lecteur, par quelque moyen que ce soit. La politique doit également minimalement contenir les informations suivantes : 8° et ss. [Reste des informations figurant à l'article 2].
À mon avis, le contenu minimal proposé par le projet de règlement est trop détaillé et ne prévoit pas d'exigence sur la durée de conservation des données recueillies. Selon le Commissariat à la protection de la vie privée du Canada (2017), une politique de confidentialité devrait contenir les éléments suivants pour permettre une décision éclairée : la personne-ressource, de l'information sur la collecte, l'utilisation, la communication et la conservation des informations, ainsi que la façon d'accéder à ces informations. En l'espèce, l'article 2 n'exige pas de spécifier la durée de conservation des données dans la politique, alors qu'elle devrait, selon moi, faire partie des exigences minimales quant au contenu de celle-ci. En contrepartie, la catégorie de personnes ayant accès aux données ainsi que les moyens utilisés pour les recueillir ne sont pas des renseignements essentiels et peuvent varier considérablement en fonction du type de données, ce qui fait en sorte que la section va être importante à titre de volume. De plus, la mention quant à la possibilité que les renseignements soient partagés à l'étranger est imprécise selon moi, puisqu'elle ne permet pas à l'utilisateur de déterminer avec certitude si les données sont effectivement transférées à l'extérieur du Québec. Aussi, considérant les préoccupations quant aux politiques trop longues qui peuvent nuire à un consentement éclairé, il serait pertinent de réduire les exigences quant au contenu. En effet, les exigences minimales pourraient servir d'excuse pour faire de longues politiques de confidentialités qui sont difficiles à suivre. Sur ce point, à cet article, j'ajouterais des restrictions globales pour faciliter la lecture d'une politique de confidentialité. Ainsi, la politique devrait être courte, posséder un vocabulaire	Je crois que certaines exigences devraient être rajoutées afin de s'assurer que le contenu d'une politique de confidentialité soit complet. D'abord, il serait bien de préciser dans la politique, le cas échéant, l'endroit où sont détenus les renseignements personnels, ce qui peut être essentiel à savoir dans le cas des établissements de santé. Le paragraphe 8(3) de Loi sur le privé prévoit déjà cette exigence pour le secteur privé. Il serait important d'aviser les utilisateurs quant à la durée de conservation de leurs renseignements personnels et à l'éventuelle destruction de ceux-ci, sur la base du principe que le consentement doit être temporaire (p. 34, Lignes directrices – Critères de validité). Le 5e principe de la LPRPDE (Annexe 1) délimite la durée de conservation des renseignements personnels. De plus, le Commissariat à la protection de la vie privée du Canada a élaboré des lignes directrices pour aider les organisations du secteur privé et les institutions fédérales à élaborer des pratiques éclairées relativement à la conservation et au retrait des renseignements personnels détenus (Conservation et retrait des renseignements personnels). Par la suite, je crois qu'une section de la politique devrait être consacrée au consentement. En effet, l'organisme mettrait de l'avant le fondement légal choisi pour collecter, utiliser ou communiquer des renseignements personnels et préciserait la forme de consentement appropriée (Lignes directrices consentement valable). Par exemple, il devrait être explicité s'il s'agit d'un consentement implicite et les raisons de ce choix (notamment si ce ne sont pas des renseignements sensibles) (p.18, Lignes directrices – Critères de validité). Enfin, la politique doit aborder les témoins de connexion

simple, être séparée en sections et favoriser des pictogrammes ou des diagrammes. De plus, l'utilisation d'une approche par niveau pour simplifier la lecture devrait aussi être préconisée.	(cookies), puisqu'ils constituent, pour la plupart, des renseignements personnels. Cette partie servirait entre autres à préciser quel type de cookies il s'agit, leur durée de vie ou pourrait simplement référer à la politique spécifique aux cookies, le cas échéant.
La difficulté concernant le contenu d'une politique de confidentialité est l'équilibre entre donner assez d'informations pour assurer la compréhension et ne pas en donner trop afin d'éviter une confusion et une lassitude. En effet, le Commissariat à la protection de la vie privée du Canada mentionne qu'afin de rédiger une bonne politique de confidentialité, le document doit être « aussi court que possible, tout en fournissant l'information dont les gens ont besoin ». De plus, la Commission d'accès à l'information du Québec, dans son rapport quinquennal de 2016 (p.76, note 248) mentionne que l'adoption de politiques de confidentialité présentées en termes clairs et compréhensibles est "une solution susceptible de répondre à [l'] exigence de transparence". En ce sens, le contenu mentionné à l'article 2 du projet de règlement semble être adéquat. En effet, les éléments demandés permettent aux consommateurs d'obtenir suffisamment d'informations, sans être déraisonnable pour les organismes. Il pourrait même être pertinent d'ajouter certains éléments, par exemple, une mention concernant la nécessité pour l'organisme public d'obtenir un consentement exprès pour certaines situations (ex : pour la communication des renseignements personnels sensibles, article 59 Loi sur l'accès). Il peut être facile pour un consommateur à la lecture d'une politique de confidentialité d'avoir l'impression que l'acceptation de la politique est une acceptation globale, un consentement à tout. Ainsi apporter des précisions sur la portée d'une acceptation de la politique augmenterait la confiance des consommateurs face à l'organisme et renforcerait leur sentiment de contrôle face à leurs renseignements personnels. Il pourrait également être pertinent d'ajouter une mention quant au délai de conservation et à la destruction des renseignements personnels par l'organisme. L'article 3.2 de la Loi sur le secteur privé mentionne cette nécessité d'encadrement quant à la conservation et à la destruction des renseignements.	L'article 2(6) du projet de règlement propose d'inclure à la politique de confidentialité les mesures à prendre pour refuser la collecte des renseignements personnels et les conséquences possibles en résultant. Cela est contraire au principe selon lequel un consentement manifeste, libre, éclairé et donné à des fins spécifiques est requis pour collecter des renseignements personnels (Lignes directrices sur le consentement de la CAI, art. 53(1) *Loi sur l'accès,* art. 14 *Loi sur le secteur privé*). Cela s'oppose également au principe de « privacy by default ». Selon ce principe, l'organisation doit s'assurer que les paramètres des moyens technologiques utilisés assurent le plus haut niveau de confidentialité par défaut, sans aucune intervention de la personne concernée (Commissariat à la protection de la vie privée du Canada, art. 63,7 *Loi sur l'accès,* art. 9,1 *Loi sur le secteur privé*). De plus, selon les lignes directrices de la CAI, le consentement doit être manifesté de façon expresse lorsqu'il s'agit de renseignements sensibles. Or, le projet de règlement ne fait aucune référence à la sensibilité des renseignements collectés. Il serait également avisé de préciser dans la politique de confidentialité qu'un organisme public peut communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques (art. 67.2.1 *Loi sur l'accès*) et de préciser dans quelles circonstances cela est rendu possible. Finalement, l'article 2(8) du projet de règlement devrait également faire mention du droit à la portabilité (art. 63,5 *Loi sur l'accès,* art. 3,3 *Loi sur le secteur privé*). Ce droit prévoit qu'un renseignement informatisé recueilli auprès de la personne concernée lui soit communiqué dans un format technologique structuré et couramment utilisé lorsqu'elle en fait la demande.
L'article 2 présente les mentions obligatoires d'une politique de confidentialité. Inclure une telle obligation dans le projet de règlement permet de créer une structure aux politiques de confidentialité, d'aider les organismes dans la	À mon avis, le contenu devant se trouver dans la politique de confidentialité n'est pas complètement bien détaillé. Nous devrions retrouver une section dans la politique faisant référence à ce qui arrive lors d'un « data breach ».

rédaction et d'éviter tout manquement. Tout comme dans le secteur on retrouve toutefois des manquements. Ces dispositions suscitent des réflexions importantes, notamment autour de l'exclusion explicite des applications, exclusion non traitée afin de se pencher sur le contenu de la politique de confidentialité. Contrairement aux lignes directrices il n'est pas clairement mentionné dans cet article les caractéristique d'écriture de la politique. Dans le secteur privé, dans un objectif de transparence et de compréhension, la politique doit être rédigée e terme simple et claire. Cette flexibilité soulève des questions quant à sa mise en œuvre pratique par les entreprises lors de la rédaction de leurs politiques de confidentialité. En effet, la nation est simplement évoquée en début sans l'accent dessus. Dans ce contexte, des déficiences peuvent émerger, entravant la pleine compréhension de l'utilisateur quant au traitement de ses données personnelles. Parmi ces insuffisances, on peut citer également citer l'incertitude quant aux délais de conservation et de destruction des données, ainsi que l'épineuse problématique de la protection des données des mineurs. En somme, l'article 2 apporte un éclairage crucial sur la structure et le contenu d'une politique de confidentialité dans un objectif de transparence et d'information. Cependant une exigence de simplicité et de clarté semblerait essentielle, les défis liés à sa mise en pratique nécessitent une attention particulière. Les entreprises devront s'efforcer de rédiger des politiques de confidentialité qui non seulement respectent la loi, mais également garantissent une compréhension aisée pour les utilisateurs, écartant ainsi les obstacles évoqués.	Considérant que le budget de sécurité varie d'une entreprise à l'autre, il me semble pertinent pour chaque organisme de bien présenter la manière dont les données seront protégées advenant le cas d'une fuite et les mesures qui seront déployées (sans toutefois dévoiler les stratégies rendant l'organisme vulnérable aux hackers). Cela permettrait à l'utilisateur de bien saisir la portée des risques auxquels il est soumis et de donner un consentement valide. Par rapport au paragraphe 7 et 8, il devrait avoir mention d'un hyperlien dirigeant directement les citoyens vers une page expliquant les étapes à prendre pour rectifier, consulter ou retirer des renseignements personnels. De plus, le paragraphe 3 manque de précision. Que veut-on dire par « les fins » ? Il me semble pertinent d'ajouter à l'article une définition qui permet de bien saisir la portée de ce paragraphe afin d'uniformiser les politiques de confidentialités. En prenant ces éléments en considération, il me semble nécessaire d'ajouter directement au projet de Règlement ou encore dans une annexe, un exemple permettant d'illustrer chaque article. Cet ajout permettrait d'atteindre l'objectif du législateur qui visait à déterminer et uniformiser le contenu des politiques de confidentialité. La politique devrait également comporter une section qui informe l'utilisateur de la publicité personnalisée et comportementale. En effet, comme il l'est indiqué par le *Commissariat à la vie privée*, ce type de publicité effectue le suivi des consommateurs afin de cibler les champs d'intérêt. Selon moi, cette mention permettrait d'informer davantage l'utilisateur sur l'information pouvant être transmise et utilisée.
Le contenu minimal d'une politique de confidentialité présenté dans le projet de règlement est pertinent mais n'est pas assez détaillé. Une publication de la CAI fournit les informations minimales que les organismes publics doivent communiquer, à partir du 22 septembre 2023, aux personnes concernées lors d'une collecte de renseignements personnels. L'objectif de la CAI est de guider les organismes publics quant au contenu de leur politique de confidentialité en attente du règlement découlant de l'article 63.4 de la Loi sur l'accès. L'article 2 du projet de règlement couvre la majorité des aspects présentés par la CAI, à l'exception des renseignements suivants : le cas échéant, la description de la technologie utilisée servant à identifier, localiser et effectuer un profilage des personnes visées ainsi que des moyens offerts pour activer les fonctions d'identification, de localisation ou de profilage ainsi qu'une mention du droit de la personne concernée de se	Le projet de règlement détaille adéquatement le contenu essentiel à une politique de confidentialité afin de satisfaire aux exigences législatives, et à permettre aux citoyens, qui répondent à leurs obligations de se renseigner, tel que confirmé dans la décision Banque de Montréal c. Bail Ltée (p. 587, 1992), de comprendre adéquatement leurs droits et l'utilisation de leurs données personnelles. Le contenu n'est pas trop détaillé, en considérant que la politique de confidentialité permet aux organisations de répondre à leur l'obligation d'informer les utilisateurs (Delwaide et Guilmain, 2016), ainsi que de mettre de l'avant le principe de transparence qui, tel que soutenu par dans les lignes directrices de la Commission d'accès à l'information du Québec, est un principe essentiel à l'obtention d'un consentement valide (p.03, Guilmain, Bigras et El Zir, 2023). De plus, dans un souci de transparence, il me semblerait même

renseigner quant à la durée de conservation des renseignements personnels. Il serait donc utile d'ajouter ces deux renseignements au contenu minimal d'une politique de confidentialité dans le projet de règlement. Aussi, l'enquête conjointe au sujet de l'application Tim Hortons réalisée par le CPVP et d'autres autorités provinciales de protection de la vie privée du secteur privé, dont la CAI, démontre que le critère de nécessité de la collecte de renseignements personnels est primordial puisque ce n'est pas toute fin qui est jugée acceptable. Selon la CAI, la nécessité est rencontrée en présence d'une proportionnalité entre l'atteinte à la vie privée occasionnée par la poursuite d'un objectif précis et les répercussions chez les personnes concernées. Il serait donc utile que l'article 2 du projet de règlement exige que les organismes publics démontrent brièvement ce test de proportionnalité dans leur politique de confidentialité. Cela militera pour une meilleure transparence et un consentement plus éclairé.	pertinent d'être informé sur la durée de conservation et la localisation des renseignements personnels. Ces informations devraient être facilement accessibles, dans une politique de confidentialité, à tous les citoyens, et ce même si la durée de conservation des renseignements se doit d'être divulguée à la demande d'un citoyen, en vertu de l'article 18 de la Loi 25, modifiant l'article 65 de la *Loi sur l'accès*. La *Loi sur la protection des renseignements personnels et les documents électroniques*, à l'annexe 1, article 4.8, implique que, selon le principe de transparence, les informations « concernant la gestion des renseignements personnels soient facilement accessibles à toute personne ». En ce sens, même si cette loi n'est pas applicable à ce projet de règlement, la durée de conservation et la localisation des renseignements personnels sont des éléments de gestion qui devrait être accessible aux citoyens.
Nous pensons que le contenu n'est pas assez détaillé. Voici notre proposition : « 1° Une mention relative au caractère facultatif ou obligatoire de la demande devra être présentée. 2° Une mention relative à l'obligation de fournir des informations supplémentaires si la collecte de renseignements se fait par des moyens technologiques comprenant des fonctions permettant d'identifier, de localiser, de profiler les utilisateurs. Il faudra aussi préciser l'obligation qui en découle qui consiste à évoquer la présence d'un paramétrage que seul l'utilisateur pourrait activer. 3° Prévenir les utilisateurs qu'il existe des domaines pour lesquels une intelligence artificielle se charge de rendre une décision. Expliquer que ceci est systématiquement précisé lors de la décision rendue et décrire les recours possibles. 4° Une mention indiquant que le consentement d'un mineur de moins de 14 ans doit être validé par un représentant légal doit apparaître. Les données personnelles des mineures ne devraient pas être traitées sans cela. 5° La gestion des incidents liés à la protection de la vie privée sera présentée ainsi que le processus permettant de traiter ces incidents. 6° Un encadrement particulier est réservé aux données biométriques. On portera une attention particulière à ces données, notamment à la reconnaissance faciale mais aussi aux données biomédicales qui sont traitées dans le système public de la santé. Le consentement exprès devrait être recueillis pour ces données et de plus, des explications concernant le stockage de ces données selon la nécessité de conservation doivent être présentées. La description des règles applicables à la conservation, à la destruction, à l'anonymisation éventuelle des renseignements	Le contenu exigé par règlement omet plusieurs questions importantes. Le paragraphe 2 devrait faire état du caractère facultatif des renseignements. Cela peut aider l'usager à prendre connaissance de ses droits en présentant l'information de manière transparente. *[…] et une mention quant au caractère facultatif des renseignements recueillis ;* Le paragraphe 3 devrait aussi exiger des organisations d'indiquer la durée de conservation des données (à titre indicatif, voir art. 53,1 al. 3 *Loi sur l'accès*), afin de faire preuve de plus de transparence, permettant à l'individu de faire valoir son droit d'accès. *[…] et la durée de conservation de ces renseignements ;* Le paragraphe 6 devrait expliciter le droit de retrait du consentement en tout temps, lorsque possible. Il s'agit d'un droit important accordé à l'usager, d'ailleurs codifié par l'article 7 RGPD visant à accroître le contrôle de l'individu sur ses propres renseignements personnels. *Le cas échéant, une mention relative au droit de retrait et […] ;* Le paragraphe 13 manque de clarté quant à la détermination de la personne ressource au sein de l'organisme. En vertu du principe de responsabilité, il serait intéressant d'exiger que les coordonnées d'une personne en particulier afin d'accroître l'imputabilité à l'interne quant aux questions relative à la politique (responsable à la PRP à l'article 8 *Loi sur l'accès*). Cela répond à la transparence du traitement des renseignements personnels au sein de l'organisation puisque les individus seront en mesure de diriger leurs questions vers une personne en particulier, qui pourra rediriger la question à l'interne au besoin. Ce fardeau ne devrait pas reposer sur les épaules d'un consommateur qui souhaite se prévaloir de

personnels doit être présentée. » Nous remarquerons que si la Loi sur l'accès ne traite pas du droit de conseil et du devoir d'assistance, le règlement n'a pas de base légale pour traiter ce sujet . Cela nous semble nuire au consentement.	services, la personne ressource citée dans la politique sera la mieux placée pour trouver la réponse à ses questions. *Les coordonnées du responsable visé par l'article 8 de la Loi sur l'accès […] ;*

2.3 Article 3 : Que pensez-vous de la collecte commune de renseignements personnels par plusieurs organismes publics ? Qui est alors responsable et détient ces renseignements (notamment en matière de respect des droits des individus, etc.) ?

La Loi sur l'accès permet à un organisme public de recueillir des renseignements personnels au nom d'un autre organisme public sous réserve des conditions prévues à l'article 64 de la Loi sur l'accès. Si un organisme public recueille par un moyen technologique des renseignements personnels uniquement pour un seul organisme public, je suis d'avis que la politique de confidentialité peut être commune. Cependant, si un organisme public recueille par un moyen technologique des renseignements personnels au nom de plusieurs organismes publics, l'organisme public qui recueille les renseignements personnels devra tenir compte de la politique de tous les organismes publics pour qui il recueille des renseignements personnels. La Loi sur l'accès ne réfère pas à la collecte commune de renseignements personnels par plusieurs organismes publics. La Loi sur l'accès réfère à la collecte effectuée par un tiers au nom de l'organisme public. La Loi sur l'accès prévoit que ledit tiers peut notamment être un organisme public. Ceci dit, je ne vois pas comment la collecte commune de renseignements personnels par plusieurs organismes publics pourraient être réalisée. Lors de la collecte, chaque organisme public devra notamment informer la personne concernée des fins pour lesquelles ces renseignements personnels sont recueillis et des conséquences pour la personne concernée de refuser la collecte de ces renseignements personnels. Puisque les fins pour lesquelles des renseignements personnels sont recueillis et les conséquences pour la personne concernée de refuser la collecte de renseignements personnels se distinguent d'un cas de figure à un autre, je vois mal comment une collecte commune pourrait être réalisée. L'organisme public pour qui les renseignements sont recueillis est responsable de la protection des renseignements personnels qu'il détient, le tout conformément à l'article 52.2. de la Loi sur l'accès.	En ce qui concerne la collecte commune des renseignements personnels, il est pertinent de se pencher sur le concept du consentement attribué à celle-ci. Dans l'éventualité où la collecte est commune, il est possible que le citoyen souhaite donner son consentement à un organisme public en particulier plutôt qu'à un autre organisme impliqué. En effet, en vertu de l'article 59 de la Loi sur l'accès, un organisme public ne peut pas communiquer un renseignement personnel sans le consentement de la personne concernée sauf dans les cas prévus par la loi. Ainsi, une disposition concernant une collecte commune de renseignement personnel sans faire mention du consentement de la personne ou de la possibilité de ne pas permettre le partage d'information en cas de refus est contradictoire avec cet article de loi. Par ailleurs, l'article 52.2 de la Loi sur l'accès fait également mention que l'organisme public est responsable de la protection des renseignements personnels qu'il détient. Dans le cas en l'espèce où il y a un partage de renseignements personnels au sein de plusieurs organismes publics, il est intéressant de se demander qui est alors responsable de la collecte et de la protection de ces renseignements personnels. En ce sens, je suis d'avis qu'il manque certaines informations quant à la responsabilité attribuée à la collecte de ces dits renseignements. Par exemple, en cas d'incidence de confidentialité au sein d'une pluralité d'organismes qui se partage les mêmes renseignements, que devrait-être la démarche à suivre et à qui revient la responsabilité ? Afin de rendre l'article 3 du projet de règlement plus précis et moins contradictoire, je propose d'ajouter la possibilité de refuser spécifiquement la collecte commune (et non pas la collecte d'informations par l'organisme public sollicité) ainsi que des précisions concernant la responsabilité en matière de respect des droits de l'individu.
La LAI prévoit, à l'article 52.2, qu'un organisme public est responsable de la protection des renseignements personnels qu'il détient. En vertu	Des précisions quant à cette possibilité de faire une politique de confidentialité commune devraient être ajoutées. L'article 3 du projet de

de l'article 8 LAI, la personne ayant la plus haute autorité au sein d'un organisme public sera responsable de la protection de ses renseignements. Il n'y a aucune précision sur la responsabilité lors d'une collecte commune de renseignements personnels. Ainsi, si deux organismes détiennent communément les renseignements, tout porte à croire qu'elles seront toutes deux responsables de leur protection. Dans le même ordre d'idée, la politique de confidentialité commune aux organismes devrait être rédigée et révisée par les organismes partenaires. Ceci pourrait avoir pour effet d'alourdir la politique de confidentialité, car chaque organisme peut avoir ses propres pratiques de gestion des renseignements personnels, ce qui pourrait doubler, tripler et ainsi de suite la quantité d'informations contenues dans la politique. Il pourrait paraître plus simple que chacune des politiques renvoie à celles des autres, mais le problème demeure ; qu'arrivera-t-il en cas de contradiction entre les différentes politiques ? Dans ce contexte, l'idée d'une politique commune est bien placée, mais encore faut-il que celle-ci soit concise et succincte pour assurer le consentement libre et éclairé. Finalement, l'article 3 du projet de règlement est possiblement incohérent avec la LAI, dans le sens où il est beaucoup moins précis que la loi habilitante. En effet, le projet édicte la possibilité d'une politique de confidentialité commune dans deux cas ; lorsque les organismes recueillent en commun des renseignements personnels et/ou lorsqu'un organisme public recueille des renseignements personnels au nom d'un autre organisme public. Toutefois, il aurait été que le projet de règlement réfère aux exceptions et conditions prévues dans la loi pour la collecte faite au nom d'un autre organisme. La disposition pourrait tout simplement référer à l'article 64, pour éviter des ambiguïtés.	règlement fait seulement référence à une collecte commune. Ainsi, cela signifie que seule la collecte se doit d'être commune pour permettre la rédaction d'une telle politique, ce qui peut être problématique quant à l'adaptation du contenu et du format. Une précision sur la façon dont le contenu doit être présenté et adapté serait donc pertinent à ajouter. Est-ce que les informations concernant les différents organismes doivent être séparées par organisme dans la politique ou s'agit-il plutôt d'énumérer l'ensemble des informations dans une seule et même section ? Comment s'assurer que les consommateurs comprennent bien, malgré une collecte commune, les distinctions pouvant exister entre les organismes (ex : fins, catégories de personnes ayant accès, mesures de sécurité) ? De plus, une précision concernant la nécessité pour chaque organisme de publier cette politique commune et de faire référence aux autres organismes et à la collecte commune pourrait être ajoutée. Une politique commune ne devrait pas faire obstacle à une rédaction en termes simples et clairs et ne devrait pas empêcher le consommateur d'avoir accès à toutes les informations dont il a besoin. Il pourrait donc être pertinent, afin d'éviter une complexité et une difficulté d'application, de se questionner quant à la possibilité de permettre une politique commune seulement lorsque les organismes ont également des finalités communes. La possibilité de ne tout simplement pas permettre une telle politique commune pourrait également être envisagée. L'article 52.2 de la Loi sur l'accès mentionne qu'un organisme public est « responsable de la protection des renseignements personnels qu'il détient ». Ce principe de responsabilité peut être perçu comme incohérent avec la rédaction d'une politique commune et de l'application d'une telle politique.
La collecte commune des renseignements personnels par plusieurs organismes publics peut s'avérer utile dans plusieurs situations. Toutefois, cette pratique devrait être mieux encadrée car elle peut donner naissance à certaines ambiguïtés quant à la responsabilité des organismes publics face à la protection des renseignements personnels qu'ils détiennent (article 52.2 de la Loi sur l'accès). Cette responsabilité implique notamment l'obligation d'ériger un processus de sécurité de l'information qui limitera les préjudices des personnes visées lors d'un incident de confidentialité. Ce processus s'articule en trois étapes, soit la prévention, la gestion et la réaction. Lors de la prévention et la gestion, les organismes qui ont recours à une collecte commune de renseignements personnels peuvent	À mon avis, si le projet de règlement entre en vigueur tel qu'il est, le fait que plusieurs organismes publics puissent collecter des renseignements personnels de manière commune sans aucune règle précise applicable au fonctionnement de leurs ententes, ce sera trompeur pour l'utilisateur. En effet, le projet de règlement ne prévoit rien outre le fait que c'est possible de le faire. Il faudrait que l'article 3 prévoit que les entités devront clairement identifier qui sera le responsable du traitement. Il faut que ce soit clair pour les utilisateurs qui détermine les finalités et les moyens de traitement. La Loi sur l'accès prévoit à son article 64 que deux organismes publics ne peuvent pas récolter des renseignements personnels de façon commune à moins que ce

s'entendre sur l'adoption, respective ou commune, des mesures qui veillent à la prévention d'incident de sécurité (par exemple, la formation du personnel de chaque établissement) ainsi que des mécanismes adéquats qui visent la protection des renseignements personnels tel que requis par l'article 63.1 de la Loi sur l'accès. Toutefois, ces délimitations de responsabilité non-officielles ont comme répercussion d'installer une grande ambiguïté quant à la marche à suivre lors de la réaction. Effectivement, lors d'un incident de confidentialité, la Loi sur l'accès impose plusieurs obligations aux organismes publics, comme le fait d'aviser la Commission et les personnes concernées en cas de risque de préjudice sérieux (article 63,8 alinéa 2). Lors d'une collecte commune, l'identification du responsable du processus réactif se complexifie et cela peut directement impacter les droits des personnes concernées. Ainsi, dans l'article 3 du projet de règlement, il serait pertinent d'indiquer la nécessité de politiques de confidentialités respectives à chaque organisme qui indique les balises claires quant au rôle de chacun à l'égard des renseignements personnels collectés. L'attribution de la responsabilité lors d'un incident de confidentialité serait alors moins ambiguë et les droits individuels seraient mieux respectés.	dernier ne collabore pour offrir des services ou qu'ils aient une mission commune. À mon avis, il transparait du texte de loi que le législateur avait un objectif de transparence. Il avait comme soucis de ne pas tromper l'utilisateur. Il est donc étrange de retrouver une disposition si peu détaillé dans le projet de règlement qui ne fait aucune mention de l'importance de la transparence et de la clarté de la collaboration entre les organismes. À titre d'exemple, l'article 26 du RGPD fait explicitement mention du fait que dans le cadre de traitement conjoint de donnée, la transparence est de mise. Ils doivent expliciter leurs obligations respectives afin d'assurer notamment le respect des droits des personnes concernées. Voici un ajout qui pourrait être fait après l'alinéa 2 de l'article 3 : « *Dans ces cas, ils sont les responsables conjoints du traitement. Ils doivent définir de manière transparente et accessibles au public leurs obligations respectives.* »
L'article 3 du règlement permet à différents organismes publics d'avoir une politique de confidentialité commune. Cela serait uniquement possible si les renseignements sont collectés dans un but commun ou au nom d'autres organismes publics. Selon la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, à son article 52.2, un « organisme public est responsable des renseignements personnels qu'il détient. » Ainsi, lorsqu'il y a plusieurs organismes publics qui conservent des renseignements personnels dans le cadre d'une collecte commune, tous les organismes qui conservent les renseignements seront responsables pour ceux-ci. Cela peut poser un problème afin de déterminer si la responsabilité en cas d'incident de sécurité est partagée, ou personnelle à chaque organisme public et pour déterminer où une plainte devrait être déposée, tel que prévu à l'article 63.3 de la *Loi sur l'accès.* Je considère que cette collecte commune de renseignements personnels pourrait aussi poser un problème concernant les procédures d'accès aux documents. Ce droit est prévu à l'article 12 de la *Loi sur l'accès.* Tel que prévu à l'article 2 al. 1(7) du projet de règlement, une personne qui consent à la politique de confidentialité peut demander à consulter ses renseignements, et les rectifier. La proposition de collecte commune pourrait rendre beaucoup plus	À mon avis, la collecte commune de renseignements par plusieurs organismes fait référence aux « joint controllers ». En vertu de l'article 26 du RGDP, cela implique qu'ils ont une responsabilité conjointe et qu'un individu va pouvoir avoir un recours contre l'un ou l'autre des organismes. Selon ce régime, les *joint controllers* devraient rédiger une entente qui spécifie les responsabilités de chacun quant au traitement des données. Dans la *Loi sur l'accès*, il n'y a pas de disposition qui prévoit expressément la possibilité de recueillir des informations de manière commune, ni que ce type de collecte est possible. Cela peut entrainer une confusion pour l'utilisateur, d'autant plus que l'article 2 du projet de règlement ne stipule pas que de telles collectes doivent être déclarées dans la politique de confidentialité. Par conséquent, cela pose un enjeu en ce qui concerne le consentement de l'usager. En effet, l'individu ne consent pas nécessairement à ce que ses renseignements soient recueillis en commun avec un autre organisme et à ce que ceux-ci soient éventuellement utilisés par celui-ci. En outre, conformément au principe de nécessité, les informations collectées doivent être nécessaires et poursuivre une fin précise, ce qui implique que les organismes devraient avoir besoin des mêmes renseignements pour les mêmes raisons afin de remplir le critère de nécessité. Or, on ne prévoit

complexe l'expérience de demande de consultation pour les citoyens. En effet, l'organisme public qui conserve les informations ne serait pas nécessairement la même que celle avec laquelle le citoyen aurait interagi. Pour ce qui est de la consultation des documents qui se fait habituellement à l'adresse de l'organisme public, en vertu de l'article 13 de *Loi sur l'accès*, les politiques de confidentialité communes pourraient causer confusion sur comment ce mécanisme s'applique dans ce cas.	pas l'éventualité où les modalités varient entre ces deux organismes. À mon avis, le projet de règlement est incomplet à cet égard. À l'article 3, je proposerais d'ajouter un nouvel alinéa qui introduit le concept de collecte commune et qui prévoit la responsabilité des organismes dans une telle situation. De plus, j'ajouterais des critères que les organismes doivent respecter pour faire une collecte commune en tenant compte des principes de transparence, de consentement et de nécessité.
La manière dont est formulé l'article 3 ne permet pas de bien saisir la portée dans laquelle une politique commune peut être utilisée. En effet, il n'y a aucune précision quant à la quantité nécessaire de renseignements personnels communs qui permet une telle politique. S'agit-il de seulement avoir une moitié de renseignements personnels communs ou les organismes doivent-ils avoir l'intégralité des renseignements personnels communs ? Toute une question s'impose quant à la responsabilité advenant le cas d'une fuite de données. L'art. 52.2 de la *Loi sur l'accès* indique que chaque organisme public est responsables des renseignements personnels qu'il détient. Toutefois, cela entre en contradiction avec l'art. 3 puisqu'une politique commune vient brouiller les cartes quant à savoir qui est le responsable du traitement et qui sont les entités sous-traitantes (pourrions-nous avoir un cas où il n'y a tout simplement pas d'entité sous-traitante et où la responsabilité est partagée (join controllership) ?). Selon moi, l'article 3 n'est pas réalisable compte tenu des contradictions, du manque de clarté et des incohérences qu'une telle pratique amènerait avec la *Loi sur l'accès*. Une alternative intéressante pourrait être celle de (1) mettre des paramètres permettant de déterminer la proportion nécessaire de renseignements personnels communs (par exemple 90-100%) (2) de permettre aux organismes publics concernés d'appliquer et d'indiquer la même section dans leur **propre politique de confidentialité** et (3) d'ajouter des hyperliens pouvant référer aux différents organismes afin d'indiquer aux citoyens que ceux-ci utilisent les mêmes renseignements personnels. Encore là, la personne doit être informée que ces renseignements personnels sont transmis à plus d'un organisme et un consentement valide doit être obtenu. Bien que 100% des renseignements soient communs, cela ne signifie pas que **toutes** les activités de l'organisme utilisent ces mêmes renseignements, d'où l'importance d'avoir une politique propre à chacun.	L'article 3 revêt une importance capitale en établissant les bases d'une politique de confidentialité uniforme en cas de politique commune. Il s'agit d'une étape cruciale pour structurer et définir les conditions régissant la gestion des données. Cette standardisation est bénéfique car elle apporte de la clarté et de la cohérence dans un domaine où les normes peuvent varier considérablement d'une entité à l'autre. Toutefois, cette disposition soulève également des préoccupations importantes. Elle omet de préciser les responsabilités en cas de collecte, de traitement, de stockage, etc. Cela crée un flou quant aux parties responsables dans différentes étapes du processus de données. En outre, il n'est pas précisé si les données sont détenues de manière commune ou séparée, ce qui peut avoir des implications significatives en matière de responsabilité et de partage d'informations. Dans le secteur privé, la situation n'est pas forcément plus claire. La loi en vigueur ne fournit pas nécessairement de directives plus détaillées concernant les responsabilités dans le contexte particulier de partage de politique de confidentialité. Cela signifie que la régulation de ces questions peut souvent reposer sur des accords contractuels entre les parties impliquées. Il pourrait être avantageux d'intégrer des dispositions spécifiques concernant la répartition des responsabilités. Une telle clarification offrirait une meilleure transparence envers les utilisateurs. En rendant les rôles et les obligations plus explicites, cela renforcerait la confiance des utilisateurs dans la manière dont leurs données sont gérées. En somme, bien que l'article 3 établisse les bases d'une politique de confidentialité commune, il reste des lacunes à combler. Il est important de définir les responsabilités de manière plus précise et de considérer la possibilité d'un traitement commun des données. La transparence envers les utilisateurs est essentielle, et cela pourrait être atteint en incluant des dispositions plus détaillées dans cette section clé.

Je trouve que l'idée de la collecte commune est un peu floue, surtout quand on aborde la question de la responsabilité et de l'imputabilité. S'il y a un incident de confidentialité, qui devra assumer tout ce qui en découle ? Selon l'article 52.2 de la Loi sur l'accès, « [u]n organisme public est responsable de la protection des renseignements personnels qu'il détient ». Dans le cas de l'alinéa 2 de l'article 3 du Règlement, l'organisme recueillant les renseignements personnels au nom des autres organismes publics sera-t-il considéré comme détenteur ? Ou est-ce que ce sera un rôle réservé aux organismes publics lui confiant la tâche ? L'article 63.8 de la Loi sur l'accès stipule que, lors d'un incident de confidentialité, l'organisme public doit prendre « les mesures raisonnables pour diminuer les risques qu'un préjudice soit causé ». Si l'incident présente un risque de préjudice sérieux, l'organisme a l'obligation d'aviser la Commission d'accès à l'information. Qui aura la tâche d'enclencher ces mécanismes dans une situation de collecte commune ? On pourrait y remédier en voyant ces situations selon l'angle *controller/processor* : l'organisme public recueillant les renseignements personnels serait le *processor*, puisqu'il le fait au profit des autres organismes publics, soit les *controllers*, qui seraient toujours responsables de leurs renseignements personnels et des incidents de confidentialité en découlant. Cela s'harmonise également avec la LPRPDE et son article 4.1.3 (Annexe 1), car « [l] » organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie. » Pour l'alinéa 1 de l'article 3 du Règlement, je propose que les organismes effectuant une collecte commune doivent procéder de la même manière que dans une relation *joint controllers*, soit décider entre eux un seul organisme qui assumera la responsabilité et qui s'occupera de la gestion des problèmes.	Chaque organisme doit avoir une personne responsable de la protection des renseignements personnel et de l'accès à l'information. Il s'agit par défaut de la personne ayant la plus haute autorité au sein de l'organisme public (*Loi sur l'accès*, art. 8). Un comité sur l'accès à l'information et la protection des renseignements personnels est également chargé de soutenir le responsable dans l'exercice de ses responsabilités et dans l'exécution de ses obligations (*Loi sur l'accès*, art. 8.1). L'élaboration d'une politique de confidentialité et le fait de veiller à son respect sont des fonctions qui incombent au responsable, aidé par le comité. Il est donc étrange de constater que le projet de règlement prévoit la possibilité d'une politique commune à plusieurs établissements. En effet, si les fonctions du responsable peuvent être déléguées à un membre de l'organisme public, un membre de son conseil d'administration, ou à un membre du personnel de direction (*Loi sur l'accès*, art. 8), elles ne peuvent être déléguées à quelqu'un d'extérieur à l'organisme. C'est pourquoi l'article 3 devrait spécifier que : « Dans le cas où plusieurs organismes ont une politique de confidentialité commune, cela n'a pas pour effet de soustraire les organismes de leurs obligations prévues aux articles 8 et 8.1 de la *Loi sur l'accès*. Ainsi, la politique doit identifier un responsable de l'accès des informations et de la protection des renseignements personnels dans chacun des organismes liés par une politique commune ». De cette façon, les personnes qui veulent se prévaloir de leur droit d'accès à l'information ou à la rectification de leurs renseignements sauront à qui s'adresser et pourront faire respecter leurs droits.
L'article 3 est plutôt simpliste, en admettant brièvement les politiques en commun selon deux cas de figure. Pourtant, la collecte par plusieurs organismes publics emporte d'importantes considérations en lien avec la protection des renseignements. Ces considérations doivent se transposer dans la politique de confidentialité, puisqu'il s'agit du moyen de communication avec le public, par l'entremise duquel le consentement est validé. Notamment, la collecte en commun vient brouiller la chaîne de responsabilité des renseignements, en contradiction avec le principe de la transparence. Il en résulte un obstacle à la compréhension du citoyen, ce qui risque de brimer son consentement éclairé. De plus, il en	Au Québec, le respect de la vie privée est un droit fondamental protégé par la *Charte des droits et libertés de la personne* et le *Code civil du Québec*. Toutefois, la collecte commune de renseignements personnels pourrait s'avérer à être un enjeu considérable, à ce droit fondamental, en lien avec la protection de certains renseignements personnels. En effet, en ce qui attrait à la responsabilité de la protection des renseignements personnels, il incombe qu' « un organisme public est responsable de la protection des renseignements personnels qu'il détient », en vertu de l'article 52.2 de la *Loi sur l'accès*. En ce sens, qu'en est-il si la collecte est commune ? À qui revient cette importante

ressort une incohérence avec l'article 63.3 *Loi sur l'accès*, qui exige une structure de gouvernance claire des rôles et responsabilités du personnel qui traite des renseignements personnels. L'incohérence découle du fait qu'on exige la publication de règles encadrant la gouvernance au sein d'une même organisation, alors qu'aucune exigence particulière ne s'impose à une politique commune. Il devient difficile pour l'individu de retracer la structure de gouvernance imputable quant au respect de ses droits. Ainsi, le règlement devrait spécifier les exigences propres d'une politique commune. Nous savons que la collecte doit faire l'objet d'une entente écrite afin d'éclairer la responsabilité des organismes. La politique devrait reprendre les termes de cette entente, notamment quant aux mesures de sécurité qui sont prévus. À défaut d'être prévu dans l'entente et à l'instar de l'article 26 (3) RGPD, la responsabilité quant aux renseignements personnels, aux droits des individus et aux mesures de sécurité devrait être solidaire. Ces mesures mettent la protection de l'individu et ses renseignements personnels au cœur de la collecte, en imposant aux organismes de se responsabiliser envers les données traitées. Ces réflexions sont aussi pertinentes et applicables au cas où un organisme public fait affaire avec une entreprise privée.	responsabilité de protection ? Désormais un responsable à la protection des renseignements personnels est désigné au sein de chacun des organismes publics et « assure le respect et la mise en oeuvre de la présente loi », en vertu de l'article 8, de la *Loi sur l'accès*. Dans le projet de règlement, on réfère même à ce responsable à l'article 2, alinéa 8, afin de fournir obligatoirement son nom et ses coordonnées au sein de chaque politique de confidentialité. En ce sens, dans le cas d'une collecte commune par plusieurs organismes publics, qui est le responsable des renseignements personnels ? La collecte commune de renseignements personnels par plusieurs organismes publics semble entrainer des incohérences au sein même du projet de règlement, et ainsi afin de clarifier les responsabilités propres à chacune des organisations, l'article 3 du projet de règlement devrait être réexaminé afin de favoriser le maintien des mesures visant la protection des données personnelles.
L'objectif de la collecte commune est certainement dans un but d'efficacité de la part des organismes publics. Toutefois, elle amène plusieurs enjeux de confidentialité. Une politique de confidentialité doit décrire le type de renseignements collectés et l'usage de ces informations et doit donc être spécifique à des fins précises. De plus, les utilisateurs consentent à avoir leurs renseignements collectés dans un but précis. Dans l'optique d'une collecte commune, il serait difficile d'obtenir un consentement éclairé sur la nature des renseignements personnels collectés, car les renseignements diffèrent grandement d'une organisation à une autre. Par exemple, les informations collectées de la part d'un CISSS diffèrent grandement de celles collectées par un CSS. Dans un premier cas, des renseignements qualifiés comme sensibles ne devraient pas être accessibles à un organisme public qui ne les recueille pas. De plus, en accord avec la Loi 25 du secteur privé et le RGPD, chaque organisme devra faire une évaluation des facteurs de risque qui varient selon la nature des renseignements collectés. Cette évaluation mène à des mesures de sécurité qui sont en respect avec la nature des renseignements personnels. De plus, certains organismes publics manipulent des renseignements personnels de nature sensible qui requiert une plus grande mesure de	Le droit à la vie privée est un droit constitutionnel protégé par les chartes. Il semble que la collecte commune de renseignements personnels est un enjeu à plusieurs égards. Nous sommes face à une sous-traitance des données. D'abord, la question de la nécessité se pose puisque les fins pourraient différer d'un organisme à un autre. Ensuite, il y a un enjeu de transparence : il semble difficile de savoir quels renseignements sont partagés avec quels organismes. De plus, lorsque l'utilisateur demande à effectuer des modifications, il faudra s'assurer que l'ensemble des organismes prennent bien en compte ces modifications. Enfin, se pose la question de l'identité du responsable de ces renseignements, de la collecte, en passant par la conservation, jusqu'à leur destruction. Puisque chaque organisme devra avoir son propre responsable de la protection des renseignements personnels, ce dernier devrait être responsable aussi de la collecte lorsque cette dernière est sous-traitée, selon le principe de l'obligation qui glisse vers la personne à qui l'on délègue la tâche. Selon la Loi sur l'accès, c'est la personne ayant la plus haute autorité au sein de l'organisme public qui reste dans les faits, responsable de la protection des renseignement personnels, malgré les chaînes de délégation que l'on pourrait rencontrer. Lors d'un incident de sécurité, l'organisme où a lieu cet

sécurité et un consentement exprès. De plus, avec une formule de collecte commune, il y a un danger pour la vie privée compte tenu du plus grand nombre de personnes ayant accès à ces renseignements. Il sera donc d'autant plus important d'avoir des mécanismes d'accès sécurisés à ces renseignements en définissant bien les personnes pouvant avoir accès aux renseignements, le cas échéant. Également, en ayant une collecte collective, il est difficile de déterminer qui est le responsable de la protection des renseignements personnels, rôle important qui est décrit par exemple, dans la Loi 25 pour le secteur privé.	incident a le devoir de communiquer l'incident à la CAI. Dans le cas de données qui ont été partagées à l'extérieur du Québec, la plus haute autorité de l'organisme est responsable du traitement et de la sécurité de ces données qui se trouvent à l'extérieur du Québec. L'organisme public devra s'assurer que l'entreprise étrangère qui possède les données personnelles de québécois les traite conformément à la règlementation québécoise. Pour ce faire, une entente contractuelle suffisamment encadrée devra être en place, comme l'a illustré l'affaire Tim Hortons.

2.4 Article 4 : Que pensez-vous de l'obligation d'un avis de modification pour toute modification (significative ou non) à une politique de confidentialité dans un délai de 15 jours ? Avez-vous des commentaires concernant le format ou les exigences y étant reliés ?

En ce qui concerne l'obligation d'un avis de modification, je suis d'avis qu'il s'agit d'une bonne idée au premier abord mais qui aurait besoin de précision. Plus précisément, pour ce qui est du délai de 15 jours, je pense qu'il s'agit d'un délai plus que raisonnable puisque ce dernier laisse le temps aux citoyens de prendre compte de cette modification. De plus, il est apprécié que ce délai ne soit pas rigide. En effet, l'option de pouvoir mettre un délai plus court si ce dernier est motivé est une bonne initiative dans une situation un peu plus urgente où la politique doit être modifiée rapidement. Cependant, je pense tout de même qu'il est nécessaire d'être plus précis concernant le genre de modification visé. Par cette disposition, je comprends que toute modification est visée par un avis de modification, mais je ne pense pas que toute modification mérite nécessairement un avis. En ce sens, les modifications purement sur la forme (modification de tournures de phrase, du format sur le site, etc.) et le changement du nom du responsable (paragraphe 13) ne devraient pas faire l'objet d'un avis de modification dans le but d'éviter une récurrence inutile de ces avis. À titre de comparaison, à l'article 8.2 de la Loi sur la protection des renseignements personnels dans le secteur privé, il est également mentionné que « toute modification » devrait faire l'objet d'un avis, ce qui constitue la même problématique qu'au niveau du projet de règlement, selon moi. Par ailleurs, il est intéressant d'observer l'article 5 du projet de règlement où il est questions de modifications significatives sans toutefois donner un exemple de ce qu'elles pourraient être. En somme, je propose que des précisions soient	Je crois que l'obligation d'un avis de modification pour toute modification, qu'elle soit significative ou non, est abusif. À titre d'exemple, je ne crois pas que cela devrait être obligatoire lorsque la modification apportée à la politique de confidentialité est de nature cléricale, laquelle ne modifie pas les renseignements personnels recueillis, les fins auxquelles les renseignements personnels sont recueillis, les catégories de personnes qui ont accès aux renseignements personnels, les moyens par lesquels les renseignements personnels sont recueillis, les coordonnées du responsable de la protection des renseignements personnels de l'organisme public, etc. Je crois que cette obligation devrait être maintenue pour toute modification qui pourrait être de nature à modifier le consentement de la personne à défaut de quoi cela nuirait à sa pertinence et entraînerait une surabondance d'avis. Je crois qu'un des objectifs de faire un avis de modification 15 jours avant l'entrée en vigueur des modifications est de permettre aux individus de retirer leur consentement, si les individus ne consentent pas aux modifications. Ainsi, je crois que l'article 4 du projet de règlement devrait préciser que l'avis de modification devrait également prévoir un paragraphe qui rappelle aux individus leur droit de retirer leur consentement ainsi que le processus de retrait de consentement.

ajoutées à cet article afin que ce ne soit pas toutes les modifications qui nécessitent un avis.	
L'article 4 demande qu'un avis soit publié avant que la politique de confidentialité d'un organisme public soit modifiée. Cet avis demande d'indiquer l'objet général des modifications, ainsi que la date d'entrée en vigueur de la modification. Cet article demande que cet avis soit publié, et ce peu importe quel type de modification il s'agit. En effet, le règlement ne fait pas de distinction entre une modification substantielle des clauses de la politique de confidentialité, et une modification de forme de cette politique. Je considère que des modifications trop fréquentes d'une politique de règlement avec différents avis et différents documents à chaque modification pourraient confondre le public, et pourrait mener à une diminution de confiance envers les organismes publics. Il serait donc pertinent d'aviser le public seulement pour les modifications substantielles. S'il s'agit d'une modification importante à la politique de confidentialité, je considère que la durée de 15 jours est trop courte pour permettre au public de réagir à cette modification. En effet, l'avis de modification doit simplement être publié, et non partagé aux utilisateurs. Ceux-ci auront donc à peine plus de deux semaines pour consulter l'avis, s'ils sont déjà au courant que celui est publié, analyser la modification et ainsi décider s'ils sont toujours confortables avec cette nouvelle politique. Ainsi, cela leur laisse peu de temps pour contacter la personne responsable de la politique de confidentialité pour soumettre des questions, ou tout autre professionnel si nécessaire, et ensuite exercer leurs droits. Aussi, le format d'une publication de l'avis sur le site Internet n'est pas suffisant pour bien informer le public. En effet, les personnes affectées ne seront pas nécessairement avisées de la publication de l'avis, et auraient encore moins de temps pour décider s'ils consentent toujours à la politique de confidentialité.	D'abord, le projet de règlement devrait, selon moi, venir baliser les raisons d'un avis de modification. Ni la LP, ni le RGPD ne prévoient des exigences quant à l'avis de modification, signifiant que l'avis doit être fait dès qu'une modification, même minime, est faite. Toutefois, selon moi, l'avis de modification ne devrait être fait que lorsque les changements pourraient venir modifier le consentement, un principe fondamental en matière de renseignements personnels. Il pourrait y avoir une norme objective pour déterminer la nécessité d'un tel avis, soit dans les cas où la modification pourrait avoir un impact sur la décision de la personne concernée de consentir à ceux-ci. Cette évaluation pourrait être du ressort de comité (art. 8.1 LAI). Autrement, l'importance de l'avis pourrait perdre son sens, si des avis de modifications sont continuellement faits, pour comme la correction d'une erreur de frappe ou pour modifier la taille ou la couleur des caractères. Deuxièmement, quant au format de l'avis, le projet de règlement prévoit que « l'objet général des modifications » doit être inscrit, ce qui est une formulation est, selon moi, trop large. Il devrait y avoir un document qui édicte clairement quels changements ont été apportés à la politique pour permettre rapidement et sans effort déraisonnable à la personne concernée d'en saisir la teneur. Par exemple, dans le domaine du droit des assurances, les modifications apportées à un contrat d'assurance terrestre sont constatées par un avenant qui est un document distinct du contrat original (article 2405 C.c.Q.). Donc, le contenu de l'avis de modification devrait être plus spécifique et préciser toutes les modifications apportées à la politique, un peu comme le fait un avenant à un contrat d'assurance. Autrement, la personne concernée devrait relire l'entièreté de l'ancienne et de la nouvelle version pour y apprendre les différences apportées.
Le règlement devrait exiger qu'un avis de modification soit publié seulement lorsque des changements significatifs sont faits à la politique. Il est déjà prévu à l'article 4(2) que l'avis doit indiquer l'objectif général des modifications apportées à la politique. L'article 5 prévoit également qu'avis de modification doit faire l'objet d'une consultation auprès du comité sur l'accès à l'information et la protection des renseignements personnels, mais seulement lorsque cet avis concerne une modification significative. Alors pourquoi l'organisme devrait-	Il est certain que cette mesure prévue par le ministère responsable de l'accès à l'information est dans le but de transparence avec les usagers de services publics. Toutefois, un avis de modification à chaque changement aura plutôt comme effet de diluer l'importance de ces changements ainsi que de confondre les utilisateurs dans leur compréhension de la politique et ainsi donc à ne pas se soucier des modifications qui pourraient avoir un impact important pour eux. Bien que la politique modifiée soit affichée sur le site internet, c'est plutôt

il publier un avis de modification pour toute modification, significative ou non ? De plus, l'article 4(2) devrait préciser que l'avis de modification doit être rédigé en termes simples et clairs, de la même manière que la politique, afin de s'assurer de la compréhension des lecteurs, comme le veut l'article 63.4 de la *Loi sur l'accès*. Finalement, pourquoi exiger un délai de 15 jours ? Sur ce point, la *Loi sur le secteur privé* (art. 8.2) ne mentionne, pour sa part, aucun délai précis à ce sujet. Voici donc la reformulation suggérée pour l'article 4 : « Lorsqu'une modification significative est apportée à une politique de confidentialité, un avis de modification de cette politique doit être publié. Cet avis doit : 1° indiquer la date de sa publication et son entrée en vigueur immédiate ; 2° indiquer, en termes simples et clairs, l'objet général des modifications apportées à la politique de confidentialité, lesquelles doivent être précisées dans une section dédiée à cette politique sur le site Internet de l'organisme public, et diffusées par tout moyen propre à atteindre les personnes concernées. »	lorsqu'il y a des changements significatifs que les utilisateurs devraient être notifiés. Il serait donc important de définir quelles sont les modifications significatives qui mèneraient à un tel avis. Le RGPD offre une explication claire d'un changement substantiel qui requiert un avis de modification, par exemple, lorsque les mesures de sécurité diminuent. De plus, quelques politiques telles que le RGPD et le CalOPPA exigent un consentement exprès à la modification substantielle d'une politique de confidentialité. Cette modalité permet de bien aviser les utilisateurs et donc favorise une meilleure transparence. Lors de changements substantiels, les utilisateurs devraient avoir accès à une façon facile de retirer leur consentement s'ils le désirent. Il est donc important de baliser la notion de modification significative pour permettre aux utilisateurs d'être avisés seulement lorsqu'il y a un impact important sur le traitement de leurs renseignements personnels. De plus, le format de l'avis de modification demeure important, car il impacte directement les utilisateurs. Les modifications à la politique peuvent être sur le site internet des services publics, mais les modifications significatives devraient être distribuées sur une plus grande échelle. Par exemple, elles pourraient être envoyées par courriel ou par un avis de type pop-up sur les applications mobiles et devront être écrites de manière claire et simple
À mon avis, ça ne fait pas de sens que le règlement ne distingue pas les différents types de modifications. Le délai de 15 jours n'est évident pas nécessaire pour une modification d'ordre clérical. Il est vrai que l'on prévoit dans le règlement que le délai peut être inférieur à 15 jours si des motifs sont invoqués. Cependant, il me semble que le législateur voulait surtout faire référence à une situation d'urgence qui nécessiterait de modifier rapidement la politique. Même si on pouvait utiliser cette exception pour les modifications de style, il ne demeure pas moins que l'obligation de consulter un comité est encore présente et cela nécessite énormément de temps et de ressources. Bref, si l'on notifie trop souvent l'utilisateur, on perdra son attention et il se lassera. En France, de nombreuses entreprises prévoient dans leurs politiques que les modifications sont effectuées sans délais et qu'elles entrent en vigueur dès leur publication, c'est le cas de France Asso Santé. Ils font notamment mention du fait que seules les modifications majeures seront communiquées et rendues disponibles pour les usagers. Il existe également des exemples d'une telle pratique au privé au Québec. C'est le cas de la politique de confidentialité du journal La Presse. L'article 12	Selon moi, l'avis de modification devrait être réservé aux modifications qui sont significatives auxquelles on réfère à l'article 5 du projet de règlement. Il conviendrait donc de définir clairement ce qu'on entend par une modification significative. Dans le RGDP, on fait plutôt référence à une modification substantielle. Pour être qualifiée de substantielle, une modification est analysée selon deux critères : l'impact de la modification sur l'individu et si le changement est inattendu pour celui-ci. Ainsi, les situations suivantes sont qualifiées comme étant des modifications substantielles : le fait d'apporter une nouvelle finalité aux données, le partage de l'information à de nouveaux tiers, des changements dans les modalités d'exercices d'un droit ou encore en cas de violation des données (Article 29 Data Protection Working Party, 2018). Ainsi, à mon avis, le projet de règlement devrait prévoir un article qui définit la « modification significative » en se basant sur cette définition du RGPD. Aussi, dans l'information devant être contenue dans l'avis, j'ajouterais la raison de la modification. Cela permettrait à l'utilisateur de mieux comprendre ce à quoi il consent. Enfin, en ce qui concerne le délai pour notifier les modifications, je crois qu'un délai de 15 jours est

prévoit que les modifications sont immédiatement applicables dès leur publication. Ils publient la version mise à jour sur leur site web et s'assurer de notifier les utilisateurs sur leur Services. Voici une version modifiée de l'article 4 : « *Un changement majeur ne peut être apporté à une politique de confidentialité avant l'expiration d'un délai de 15 jours à compter de la date de publication d'un avis de modification de cette politique […]. Constitue un changement majeur tout changement qui aura pour effet d'invalider le consentement manifeste, libre et éclairé d'une personne concernée.* »	très contraignant pour les organisations et peut même nuire aux consommateurs. En réalité, il me semble préférable de permettre aux organisations de mettre leur politique de confidentialité le plus à jour possible. Cela pourrait être particulièrement problématique en cas de fuite de données où l'organisme doit modifier sa politique subséquemment. Même si on peut y déroger en joignant les motifs à l'avis une formulation comme celle de « dans les plus brefs délais » serait plus appropriée. Elle permettrait à l'utilisateur d'être suffisamment informé sans restreindre les activités de la compagnie de manière excessive et donc de maintenir un équilibre entre ces deux intérêts.
L'article 4 du projet de règlement ne fait pas référence au type de modifications entrainant l'obligation d'un avis de modification, contrairement à l'article 5 al.2 qui mentionne que seules les modifications significatives à une politique doivent faire l'objet d'une consultation. Ainsi, l'absence de précision quant à la nature de la modification (significative ou non) permet d'en déduire que toutes les modifications entrainent une obligation d'avis. Il semble irréaliste et surtout non nécessaire de demander aux organismes de publier un avis de modification pour tous types de modifications. Considérant les objectifs d'une politique et des avis pour les citoyens (harmonisation des politiques, compréhension de leurs droits et utilisation des renseignements personnels), il ne semble pas pertinent pour ces derniers d'être mis au courant de chaque modification non significative d'une politique (ex : orthographe, mise en page, changements mineurs n'affectant en rien le fond de la politique). Ainsi, il pourrait être pertinent de préciser que seules des modifications significatives, ou du moins des modifications en lien avec le contenu même de la politique, doivent faire l'objet d'un tel avis. Par la suite, il est possible de se questionner quant à la nécessité d'un délai de 15 jours entre la publication de l'avis et la modification de la politique. En effet, pour qu'un tel délai soit utile, les consommateurs doivent être en mesure de voir l'avis, et ce, dès le début du délai. Cependant, un tel avis, publié sur le site Internet de l'organisme, ne sera réalistement pas vu par tous les consommateurs 15 jours avant la modification de la politique, et même s'il est vu par certains, ceux-ci le verront probablement dans un délai moindre, voire le jour même de la modification ou après. Cette difficulté pratique rend abstrait la pertinence d'avoir un tel avis.	D'abord, je crois qu'il serait pertinent qu'il soit indiqué les raisons du changement de la politique de confidentialité. Ainsi, je rajouterais cette exigence à l'article 4 du Règlement. Ensuite, il est important de se poser la question de ce qui nécessite d'être avisé. Le secteur privé prendra la même approche que le Règlement : l'article 8.2 de la Loi sur le privé stipule qu'un avis doit accompagner toute modification faite à la politique de confidentialité. Néanmoins, est-ce que toutes les modifications sont valables ? Pas nécessairement, à mon avis. Par exemple, si on change une simple virgule, un avis ne s'avère peut-être pas essentiel. En même temps, si ce changement de virgule transforme le sens de la phrase complètement, il peut être intéressant d'aviser les utilisateurs. Le RGPD, quant à lui, énonce qu'il y a une obligation d'informer lors d'une modification substantielle ou d'un événement particulier (RGPD - CNIL). Il serait possible de transposer ce concept en droit québécois, puisque, selon moi, il s'agit d'une manière de faire beaucoup plus efficace, afin d'éviter la multiplication des avis. Donc, j'ajouterais à l'article que l'avis est nécessaire dans le cas d'une modification substantielle de la politique de confidentialité, soit lorsqu'on change l'essence de la politique ou de ses composantes. En somme, l'article 4 ressemblerait alors à ceci : « Une politique de confidentialité ne peut être modifiée de manière substantielle avant l'expiration d'un délai de 15 jours à compter de la date de publication d'un avis de modification de cette politique ou, le cas échéant, avant l'expiration d'un délai plus court mentionné dans cet avis de modification […] 5° indiquer les raisons des modifications apportées. »

Je suis d'avis que les modifications significatives, tel qu'un changement au niveau des fins de collecte ou des moyens de collecte se doit d'être signalés aux citoyens et à mes yeux, il faudrait également exiger aux organisations publics de fournir la raison de la modification à une politique de confidentialité (ex. changements législatifs). En vertu, de l'article 19 de la *Loi 25* insérant l'article 65.0.2 à la *Loi sur l'accès*, une politique de confidentialité, ainsi que son contenu, agit à titre de consentement pour l'utilisation et la communication des renseignements personnels. En ce sens, afin de mettre de l'avant le principe de transparence et de permettre un consentement éclairé, les citoyens devraient être avisés des modifications significatives et de la raison de la modification à la politique. Toutefois, il ne s'avère pas nécessaire, à mes yeux, d'aviser les citoyens pour toutes les modifications (non significatives). Il serait préférable de s'inspirer des mesures comprises dans le *règlement général sur la protection des données* (RGPD) qui implique d'informer les gens seulement lors de modifications substantielles ou d'évènement particulier, incluant une nouvelle finalité ou un nouveau destinataire (CNIL, 2019). De plus, je considère que le délai de 15 jours entre l'avis de modification et la modification de la politique de confidentialité n'est pas nécessaire, plus particulièrement parce que ce délai peut être modifié par une simple notification du motif par une organisation et qu'il n'est pas exigé dans le secteur privé, en vertu de l'article 107 de la *Loi 25* modifiant l'article 8.2 de la *Loi dans le secteur privé*. En ce sens, la politique devrait être modifiée rapidement afin d'être conforme aux pratiques actuelles de collecte de renseignements personnels.	Le projet représente une avancée significative en matière de transparence en imposant la publication d'un avis à chaque modification de la politique de confidentialité. Cette disposition vise à informer les utilisateurs sur les changements apportés au traitement de leurs données personnelles. Bien que cette initiative soit louable, il est important de considérer si la publication systématique d'avis à chaque modification est réaliste et si elle peut maintenir son objectif de transparence à long terme. L'idée de publier un avis pour chaque modification peut sembler idéale pour garantir une totale transparence. Cependant, il est essentiel de prendre en compte le risque de surnombre. Trop d'avis de modification pourraient finir par agacer les utilisateurs, les désensibilisant potentiellement à l'information vitale que ces avis cherchent à communiquer. Cette saturation pourrait aller à l'encontre de l'objectif initial de transparence et de protection des droits des utilisateurs. Une alternative pourrait être de suivre l'exemple RGPD, qui exige la publication d'avis pour les modifications substantielles et significatives. Cette approche permettrait de préserver l'essence de la transparence tout en évitant la surcharge d'informations pour les utilisateurs. Ainsi, les modifications mineures de forme pourraient être exclues de cette obligation de publication d'avis, se concentrant plutôt sur les changements qui ont un impact réel sur la manière dont les données personnelles sont traitées. Le préavis de quinze jours n'est pas présent dans les autres réglementations et peut sembler utile. Ce préavis peut sembler nécessaire pour la transparence mais une tache administrative futile. En fin de compte, il est primordial de trouver un équilibre entre la volonté de transparence et la nécessité de ne pas submerger les utilisateurs d'informations. Une réflexion approfondie sur la portée des avis et leur fréquence est nécessaire pour que cette disposition puisse réellement servir les intérêts des utilisateurs tout en demeurant pratique et efficace.
Selon moi, l'article 4 n'est pas adéquat. D'emblée, cet article présente un manque de précision quant au terme « modification ». Il est difficile de savoir de quel type de modification il est question. S'agit-il d'un déplacement de virgule, d'un changement de modalité complet ou d'un incident de confidentialité ? Cet article devrait comporter une définition du terme modification en y apportant également la mention « modification pertinente ». Envoyer un avis à tous les utilisateurs dès lors d'une simple modification de syntaxe n'est pas pertinent et viendrait engorger les notifications des	À mon avis, la publication d'un avis de modification n'aurait pas toujours à respecter un délai de 15 jours. La question d'avis de modification est intrinsèquement liée aux exigences de consentement des personnes concernées. Dans la Loi sur le secteur privé, l'article 14 établit que le consentement valide à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Dans la LPRPDE, le consentement peut être explicite ou implicite et, d'après l'article 6.1, sa validité repose sur la raisonnabilité de conclure à

utilisateurs en enlevant de l'importance pour les modifications qui sont réellement pertinentes et qui modifie la politique de confidentialité. J'aperçois également un manque de précision quant à la méthode de notification. Parlons-nous ici d'un avis en accédant au site Internet à la page d'accueil, directement sur la politique de confidentialité ou encore d'une notification par courriel ? Il serait pertinent d'ajouter un mode de transmission d'avis au Règlement afin d'assurer de respecter les objectifs de celui-ci (uniformisation). Le Règlement ne prend également pas en compte les applications dans le moyen de donner l'avis (comment cela fonctionnerait-il ?). Il devrait également y avoir un tableau (qui pourrait être référé via un hyperlien de la section des modifications) indiquant les modifications jugées non pertinentes (selon les modalités instaurées par le Règlement, comme la syntaxe) à la notification afin de garder une transparence avec les utilisateurs et de respecter leur droit à l'information. Le secteur privé devrait également être inclus dans cette observation du moyen de transmission de l'avis lors d'un incident de confidentialité. Pour le délai de 15 jours, je crois qu'il devrait être adapté en fonction de la modification. Pour les modifications « non pertinentes », il pourrait y avoir un délai plus grand de 30 jours par exemple.	la compréhension par la personne concernée de la nature, des fins et des conséquences de la collecte, de l'utilisation ou de la communication de ses renseignements personnels. Le caractère commun de ces dispositions est l'importance qui est donnée à la compréhension des fins visées au moment du consentement. Par ailleurs, l'article 65,1 alinéa 1 de la Loi sur l'accès établit aussi qu'un renseignement personnel ne peut être utilisé au sein d'un organisme public qu'aux fins pour lesquelles il a été recueilli (sauf exceptions). Ainsi, il serait primordial de demander le consentement des personnes concernées dès lors que les fins visées au moment du consentement initial changent d'une quelconque manière (ce qui constitue une modification significative). À mon avis, les fins constituent les aspects relatifs à la manière de collecter, d'utiliser et de communiquer les renseignements personnels. Ainsi, il serait utile de faire la nuance à l'article 4 du projet de règlement entre les changements apportés aux fins visés par le consentement initial (auquel cas un avis de modification dans un délai de 15 jours serait publié pour permettre la réévaluation du consentement des personnes concernées) et les autres changements apportés (auquel cas l'avis serait émis simultanément avec la nouvelle version de la politique de confidentialité).
En comparant aux autres lois applicables (PIPA BC/Alberta, PIPEDA, RGPD), aucune autre législation n'impose d'obligations aussi étendues. Il s'agit d'une exigence qui risque de noyer les citoyens dans une marée d'avis parfois superflus. Si les organisations devaient aviser les usagers de toute modification à la politique de confidentialité, cela risque d'entraîner une lassitude ou une indifférence chez l'individu, qui ne sera plus en mesure de distinguer les modifications importantes des modifications de forme. Il aurait été préférable d'exiger un avis que lors d'une modification substantielle ou lorsqu'elle impacte le consentement obtenu chez l'individu. En effet, selon les Lignes directrices du WP29, en accord avec les principes de loyauté et de transparence, les organismes doivent tenir compte des attentes raisonnables de l'individu, ou encore de l'impact potentiel des changements sur l'intéressé (par. 30). Ces nuances méritent d'être codifiées afin de distinguer les modifications justifiant un avis des modifications mineures (ex. de forme), qui peuvent simplement être temporairement mis en évidence dans la politique de confidentialité. L'argument va de même pour le délai de préavis. En appliquant l'article à toute modification, un organisme devrait attendre 15 jours pour modifier une	Nous pensons que l'avis de modification ne devrait concerner que les modifications de fonds. Actuellement, il y a un risque que cela nuise à l'efficience des organismes publics pour lesquels une pénurie de personnel existe. Nous trouvons que le délai de 15 jours est court, il ne favorise pas les possibilités de réactions. La loi sur le secteur privé fait preuve de neutralité technologique. Au niveau Européen, le RGPD impose l'aval du comité lorsque les modifications de la politique de confidentialité touchent les données personnelles. De plus, une consultation des parties intéressées et des personnes concernées devraient être réalisée lorsque cela est possible. Proposition : Une politique de confidentialité ne peut être modifiée avant l'expiration d'un délai de 30 jours à compter de la date de publication d'un avis de modification de cette politique ou, le cas échéant, avant l'expiration d'un délai plus court mentionné dans cet avis de modification. Seules les modifications de fond sont concernées par ce présent article. L'avis de modification doit : « 1° indiquer la date de sa publication ; 2° indiquer l'objet général des modifications apportées à la politique de confidentialité, lesquelles doivent être précisées dans une section dédiée à cette politique sur le

coquille ou les coordonnées du responsable dans sa politique. Il est donc souhaitable de réserver l'exigence d'un préavis aux modifications substantielles tel qu'exposée ci-haut. Au surplus, selon le WP29, le paragraphe 2 devrait exiger que l'organisme fasse état de l'impact des changements sur les individus, suivant le principe de loyauté (par. 31). Ce faisant, les individus seront en mesure de déterminer les finalités et les raisons du changement apporté. *Une politique qui fait l'objet d'une modification substantielle, de manière à altérer le consentement de la personne concernée, ne peut être modifiée avant l'expiration d'un délai […] Cet avis doit :* *[…] Indiquer l'objet général des modifications et les conséquences possibles en résultant.*	site Internet de l'organisme public, et portées à la connaissance de toute personnes concernées par tout autre moyen ; 3° indiquer la date de l'entrée en vigueur des modifications ; 4° si l'avis mentionne un délai plus court que le délai de 30 jours, les motifs qui justifient cette dérogation doivent avoir un caractère impératif et être présentés. 5° Une consultation de l'ensemble des parties devrait être réalisée et les opinions devraient être prises en considération ; 6° Avant publication, toute modification doit avoir été approuvée par le comité sur l'accès à l'information et la protection des renseignements personnels. »

2.5 Article 6 : Que pensez-vous de la méthode de publicisation d'une politique de confidentialité et de l'avis de modification ?

L'article 6 du projet de règlement exige que la politique de confidentialité et l'avis de modification soient publiés dans une section dédiée à cette politique sur le site internet de l'organisme public. Premièrement, cet article serait plus cohérent avec la Loi sur l'accès, plus spécifiquement l'article 63.4 de la Loi sur l'accès, si la politique et l'avis de modification étaient également diffusées « par tout moyen propre à atteindre les personnes concernées ». Deuxièmement, l'expression « section dédiée » manque de clarté. Je crois qu'exiger que la politique soit publiée sur le site internet de l'organisme public et qu'elle soit facilement accessible à partir de la page d'accueil du site, serait suffisant. L'article 6 du projet de règlement exige aussi qu'une version antérieure de la politique soit publiée dans la même section que la version en vigueur. Bien que le législateur précise dans cet article que l'organisme public doit veiller à ce que la version antérieure ne soit pas confondue à la version en vigueur, je crois que maintenir les deux versions sur le site internet de l'organisme public suscitera plus de confusion que de clarté.	L'article 6 du projet prévoit que la politique de confidentialité et l'avis doivent être publiés dans une section dédiée à cette politique sur le site Internet de l'organisme public. Je pense que cette exigence permet à une personne d'accéder plus rapidement et facilement aux informations concernant les pratiques de l'organisme. Toutefois, l'article pourrait être plus précis et ajouter une exigence en lien avec la facilité d'accès de cette section. Il pourrait s'agir d'une norme objective inspirée de celle qu'intègre la LPRPDE à son huitième principe, avec la notion des efforts raisonnables. Ensuite, l'article 6 prévoit la conservation de la plus récente version antérieure et d'une version nouvelle de la politique. Dans l'optique où l'avis de modification pourrait être transmis seulement en cas de changements significatifs, je pense qu'il pourrait être pertinent pour l'organisme, pendant un certain délai, de conserver toutes les versions antérieures de ses politiques dans une catégorie d'archives. Cet historique permettrait de garder des traces de toutes modifications, même pour des changements mineurs, en guise d'alternative à l'envoi d'un avis pour tout type de modification. La LAI, quant à elle, à son article 63.4, donne l'obligation pour l'organisme public qui récolte des renseignements personnels par moyen technologique, la publication sur le site Internet et la diffusion par tout moyen propre à atteindre les personnes concernées. La LP (article 3.2) prévoit aussi la publicisation sur le site Internet de l'entreprise ou « par tout autre moyen approprié ». Dans le RGPD (article 12), il est prévu que le responsable du traitement fournisse toute information relative à la politique par les

	moyens appropriés, par écrit ou par voie électronique. Alors, pour assurer une meilleure cohérence, il serait bien que le projet de règlement reprenne simplement à son article 6 les termes utilisés dans la LAI.
À mon avis, l'exigence qui veut que la politique de confidentialité d'un organisme doive être publiée sur son site internet dans une section dédiée est trop restrictive. En effet, cette disposition n'applique pas le principe de la neutralité technologique qui prévoit que les lois et règlements ne devraient pas préférer une technologie par rapport à une autre pour atteindre un objectif donné (De Rico, J.-F. et Jaar, D., 2008). Or, selon l'article 6, une politique de confidentialité accessible sur une application, par courriel électronique ou encore envoyé par la poste ne serait pas suffisante pour être conforme à la loi. Étant donné que le projet de règlement cherche à établir des exigences minimales, il semble déraisonnable d'imposer un format aussi précis pour la publication de la politique de confidentialité. C'est d'ailleurs une exigence qui est, pour le moment, spécifique au secteur public, car à l'article 8.2 de la *Loi sur le secteur privé*, on prévoit que les entreprises peuvent utiliser d'autres moyens si elles ne disposent pas d'un site internet, et la loi ne requiert pas de section dédiée à la politique de confidentialité. Dans le RGDP, on spécifie à l'article 12.1 que la politique doit être transmise par écrit, mais on ne prévoit pas un moyen particulier. À mon sens, il serait préférable de ne pas imposer un format spécifique, mais plutôt d'exiger que la politique soit facilement accessible et qu'elle soit disponible par écrit. Par exemple, l'avis de modification pourrait être transmis par courriel sans nécessairement figurer sur le site internet. En outre, je crois que l'article ne devrait pas exiger de publier les versions antérieures dans la section dédiée. J'ajouterais plutôt une disposition voulant que l'organisation mette les versions antérieures de la politique de confidentialité à disposition sur demande.	Je crois qu'il s'agit d'une mauvaise idée de spécifier que la publicisation doit se faire spécifiquement sur le site Internet. En effet, il est important de faire preuve de neutralité technologique. Par-là, j'entends que cette disposition semble exclure d'autres supports technologiques (ou non-technologiques, comme la poste), notamment les applications. Nous pouvons penser à l'application d'Hydro-Québec (qui est assujetti à la Loi sur l'accès) : est-ce que cela signifie que celle-ci n'est pas dans l'obligation d'avoir une section distincte pour sa politique de confidentialité ? Est-ce que l'utilisateur qui a recours uniquement à l'application pourra facilement accéder à la politique ou sera avisé de ses modifications ? Il serait mieux d'adopter une approche plus neutre. À titre d'illustration, l'article 8.2 de la Loi sur le privé énoncera bientôt que l'entreprise devra « […] diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs. » Également, à l'article 12 du RGPD, on précise plus largement que « [l]es informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. » Selon les principes de la LPRPDE (Annexe 1), la notion de publicisation est encore plus étendue : « Une organisation peut rendre l'information concernant sa politique et ses pratiques accessibles de diverses façons. La méthode choisie est fonction de la nature des activités de l'organisation et d'autres considérations » (4.8.3). Dans le même esprit, je crois qu'il faudrait modifier le premier paragraphe de l'article 6 du Règlement afin de faciliter les choses et de permettre une harmonisation : « Une politique de confidentialité et un avis de modification doivent être publiés dans une section dédiée à cette politique sur le site Internet de l'organisme public et diffuser par tout moyen propre à atteindre les personnes concernées. »
Par souci de cohérence avec la Loi sur l'accès (art. 63.4), il serait pertinent d'ajouter au projet de règlement une précision quant à la diffusion d'une politique. En effet, la loi prévoit qu'une telle politique doit être publiée sur le site Internet et diffusée « par tout moyen propre à atteindre les personnes concernées ». Le gouvernement du Québec a précisé que cette mention de « tout moyen propre » signifie, entre autres, qu'un	Il est certain que l'obligation de publier la politique de confidentialité ainsi que tout avis de modification dans une section dédiée à cette politique sur le site Internet de l'organisme public est une bonne méthode de publicisation afin de rendre l'information qu'elle contient plus évidente. Toutefois, il serait intéressant que le libellé de la disposition mette l'emphase sur l'importance d'attirer l'attention des personnes

organisme public qui conçoit une application doit rendre accessible sa politique sur cette application. De même qu'un organisme qui offre un produit technologique devrait affichée sa politique sur l'emballage ou les instructions du produit. Clarifier ce point directement dans le règlement permettrait non seulement de préciser la signification de « tout moyen propre », mais également de rendre l'article 6 du règlement cohérent avec l'article 63.4 de la loi, l'article 6 faisant seulement mention d'une publication sur le site Internet. Il pourrait également être pertinent d'ajouter une précision quant à la méthode de publicisation de l'avis de modification. En effet, afin d'avoir un effet véritable, l'avis doit être en mesure d'être vu par les consommateurs. Toutefois, si par exemple l'avis est publié au même endroit que la politique, il y a davantage de risques que celui-ci ne soit pas vu. Un consommateur qui a déjà lu la politique de confidentialité ne va pas retourner régulièrement sur la page où la politique est publiée et ne verra donc pas l'avis qui s'y trouve également. Il serait alors possible de mentionner dans le projet de règlement qu'un tel avis doit obligatoirement être affiché sur la page d'accueil du site et de façon distincte de la politique confidentialité.	concernées ainsi que le fait que la politique doit être accessible sans effort déraisonnable. En effet, même si la politique est bel et bien publiée dans une section dédiée à celle-ci, il serait contreproductif que cette section soit difficilement accessible (par exemple, qu'il faut cliquer à plusieurs endroits afin d'y accéder). À son article 4.8.1., la LPRPDE fait également mention du principe de transparence en mentionnant qu'une personne doit pouvoir obtenir sans efforts déraisonnables de l'information auprès de la politique d'une organisation. Bien qu'il s'agisse d'une loi qui s'applique au secteur privé, le même principe s'applique en ce qui concerne la publicisation d'une politique ainsi que son avis de modification des organismes publics. Par ailleurs, dans le mémoire écrit par le Ministre responsable de l'Accès à l'information, il a été mentionné que lors de la collecte de renseignements personnels, les organismes publics devraient attirer l'attention de la personne concernée sur la politique de confidentialité et sur l'avis de modification avec l'aide, par exemple, d'un bandeau lorsque la personne accède au site Web. Ainsi, il est bien que la politique de confidentialité ait sa propre section sur le site internet de l'organisme, mais il faudrait attirer l'attention de la personne concernée vers cette politique et rendre son accès facile et évident. Afin d'améliorer la méthode de publicisation, je propose que l'article 6 accorde davantage d'importance à la facilité d'accès des politiques de confidentialité.
Le projet de règlement est légèrement défaillant à cet égard. En effet, si l'on garde en tête l'objectif visé par le législateur, soit d'harmoniser les pratiques en matière de politique de confidentialité afin que l'utilisateur s'y retrouve mieux, il semble contre intuitif d'obliger la publication des politiques et des avis uniquement sur le site internet des organismes publics. Plusieurs entreprises privées au Canada et ailleurs (voir : McDonald's, 3M France etc.) ne prévoit que cette manière de publicisation et je trouve cela problématique. Ça impose un important fardeau à l'utilisateur, qui doit constamment s'assurer d'être au courant de la dernière version. À mon avis, pour régler ce problème, il aurait plutôt fallu lire l'article 6 ainsi : « *Une politique de confidentialités et un avis de modification doivent être rendus accessible au public par quelque moyen que ce soit.* » De cette façon, on s'assure de tout inclure les moyens possibles de publier. Cela fait écho au concept de l'équivalence fonctionnelle, difficilement dissociable du principe de neutralité technologique, puisque tant que l'objectif est atteint, soit de communiquer la politique de confidentialité aux utilisateurs, le moyen choisi	La politique de confidentialité ainsi que l'avis de modification devraient être accessibles par d'autres formats de publicisation. Si nous nous attardons à la LPRPDE, l'article 4.8.3 de l'annexe 1 mentionne que lorsque les organisations s'acquittent de leur devoir de transparence à l'égard du public, elles peuvent rendre l'information concernant leurs politiques et leurs pratiques en matière de renseignements personnels accessible de diverses façons et que la méthode doit être choisie en fonction de la nature des activités de l'organisation et d'autres considérations. D'ailleurs, le Commissariat à la protection de la vie privée du Canada recommande d'utiliser diverses manières d'accessibilité de l'information. À titre de deuxième exemple, l'article 8.2 de la Loi sur le secteur privé qui est rédigé de la même manière que l'article 63.4 de la Loi sur l'accès fait référence à la publication de la politique de confidentialité et à son avis de modification sur le site Internet de l'entreprise et aussi à leur diffusion par tout moyen propre à atteindre les personnes concernées. Ainsi, la LPRPDE et la Loi sur le secteur privé s'entendent sur le fait de prioriser la publication de l'information en utilisant

pour le faire importe peu. Il se peut que pour certaines personnes, il soit plus facile de lire et d'accéder à une politique de confidentialité version papier. Il pourrait également être intéressant, par exemple, de rendre les politiques de confidentialité disponible sur les réseaux sociaux des organismes publics, question d'atteindre le plus grand nombre d'utilisateurs possible. De plus, le fait d'ajouter cette mention à l'article 6 nous permet d'avoir une loi qui évoluera dans le temps. Cela donnera une plus ample amplitude d'interprétation. Par exemple, la politique de confidentialité du journal La Presse prévoit ce mécanisme. En effet, le journal peut rendre accessible une modification à sa politique directement via ses Services ou par d'autres moyens.	divers formats qui s'arrimeront avec la nature des activités de l'organisme de sorte à pouvoir atteindre de manière efficace les personnes concernées. À mon avis, la Loi sur l'accès ne fait pas exception à cette interprétation des moyens de publicisation, d'autant plus que son article 63.4 est rédigé de la même manière que l'article 8.2 de la Loi sur l'accès. Il serait donc utile qu'à l'article 6 du projet de règlement, d'autres formats de publicisation soient rajoutés et que ceux-ci soient cohérents avec l'aspect technologique de la collecte des renseignements personnels par l'organisme public. Ces autres méthodes pourraient être l'envoi de courriers électroniques ou bien de notifications par téléphone aux personnes concernées.
La publicisation d'une politique de confidentialité en ligne, sur le site internet, est en respect avec les indications de la loi sur le secteur privé, celle du RGPD ainsi que l'art 63.4 de la LAI. Toutefois, la notion de « diffuser par tout moyen propre à atteindre les personnes concernées » de l'art 63.4 de la LAI porte à croire que le site internet de l'organisme public ne suffirait pas pour rejoindre le plus grand nombre d'utilisateurs. De ce fait, compte tenu de la nouveauté de cette réglementation, d'autres moyens pourraient être utilisés pour rejoindre un plus grand nombre d'utilisateurs, tel que par courriel lors de la publication originale de la politique de confidentialité. Également, pour la publication internet, il serait pertinent d'avoir un accès facile à la politique, par exemple mettre un onglet « protection de votre vie privée » directement sur la page d'accueil, car il est souvent difficile de trouver une politique de confidentialité directement sur le site internet d'une entreprise. De plus, si les organismes publics utilisent des applications mobiles, la politique pourrait également se retrouver sur la page d'accueil de l'application dans le but de rejoindre un plus grand nombre d'utilisateurs. Concernant l'avis de modification, la Loi 25 pour le secteur privé et pour le secteur public note que l'avis doit être publié sur le site internet de l'entreprise ou de l'organisme. Pour permettre de rejoindre un plus grand nombre d'utilisateurs, l'avis pourrait également être diffusé de plusieurs façons tel qu'en pop-up ou bannière lorsque l'utilisateur se connecte sur l'application où lorsqu'il entre sur la page internet de l'organisme. De plus, des notifications directes aux usagers telles que des envois courriel permettraient d'aviser les utilisateurs de modifications importantes à la politique de confidentialité. Il	La méthode de publicisation prévue à l'article 6 du règlement prévoit que la politique de confidentialité et les avis de de modifications doivent être publiées sur le site Internet de l'organisme public. Je considère que cela peut poser certains problèmes. En effet, le fait que les documents soient simplement publiés sur Internet, sans avertir les utilisateurs, peut rendre plus difficile son accès. Par exemple, certaines personnes plus âgées, ou sans connexion à l'Internet, pourraient ne pas avoir accès à la politique de confidentialité. L'article 4.8.1 de la *PIPEDA*, demande que les citoyens aient accès aux politiques sans effort déraisonnable. L'article 4.8.3 de cette loi, permet que la publication des politiques soient accessibles par différents moyens, tel que par téléphone, par brochure, ou par envoi par la poste. Cela permet que la population ait un meilleur accès aux informations, ce qui est particulièrement important lorsque nous sommes dans le secteur public. L'article 63.4 de la *Loi sur l'accès* demande que la politique de confidentialité et l'avis de modification de la politique soit diffusé par tout moyen pour atteindre les personnes concernées. L'article 8.2 de la *Loi sur la Protection des renseignements personnels dans le secteur privé* donne une obligation similaire. En prenant cela en compte, le fait de simplement publié sur un site Internet l'avis ne serait pas nécessairement suffisant pour que toutes les personnes concernées aient accès à la modification, puisqu'une personne normale ne va pas nécessairement vérifier les sites internets des organismes publics avec lesquels ils interagissent régulièrement. Le règlement demande que les anciennes versions des politiques soient disponibles. Cela permet au public de comparer la nouvelle version et les anciennes versions. De ce

faudrait d'abord déterminer à quel moment une modification devient assez importante pour un tel envoi.	fait, si l'avis porte à confusion sur les modifications apportées à la politique de confidentialité, il sera possible de les évaluer d'une autre façon.
Avec ce projet de règlement apparait une obligation de publicisation d'un avis de modification au utilisateur en cas de modification de la politique de confidentialité de l'organisme. Cet avis a pour objectif plus de transparence envers les utilisateurs et une meilleure protection et compréhension des données personnelles. Toutefois, est seulement imposé d'inclure cet avis dans la même section que la politique elle-même. Cela laisse aux organismes une plus grande latitude pour décider comment communiquer ces changements à leurs utilisateurs. Pour aviser les utilisateurs, plusieurs options pourrait être envisageables. Un bandeau sur le site offre une grande visibilité mais risque de passer inaperçu ou peut sembler inapproprié sur une première page de site web. Un email peut être contraignant, mais est plus direct et garantit une notification personnelle. Cependant, il peut également être perçu comme intrusif. Il peut alors, tel que prévu dans le projet envisager un simple avis sur la page de la politique de confidentialité, mais pourrait aller à l'encontre de la volonté d'une stricte transparence. Une demande d'acceptation explicite est une méthode rigoureuse mais complexe à mettre en place. Elle assure que les utilisateurs sont informés et donnent leur consentement actif avant de continuer à utiliser les services, mais peut entraîner une baisse du taux d'acceptation. Elle peut être toutefois sembler nécessaire en cas de renseignements sensibles. La question centrale reste celle de l'utilité de la notification de médication notamment en cas de modification subsidiaire de la politique de confidentialité. Choisir la méthode d'avertissement dépendra du contexte, des préférences de l'organisme et de la sensibilité des modifications apportées à la politique de confidentialité.	À l'heure actuelle, le projet de règlement prévoit que la politique et l'avis de modification doivent être publiés dans une section dédiée sur le site Internet de l'organisme (art. 6). Ils doivent également être portés à l'attention de la personne « [l]ors de la collecte de renseignements personnels » (art. 7). Le législateur aurait pu s'inspirer de l'article 8.2 de la *Loi sur le secteur privé* et exiger des organismes qu'ils diffusent également leur politique de confidentialité « par tout moyen propre à atteindre les personnes concernées ». Cela encouragerait les organismes à faire preuve de créativité afin de rendre le contenu plus facilement accessible à un plus grand nombre. Le projet de règlement pourrait également s'inspirer des conseils du Commissariat à la vie privée du Canada : « Ne vous arrêtez pas à placer votre politique sur votre page d'accueil, donnez de plus amples renseignements en publiant des avis "juste à temps" (p. ex. intégrez des hyperliens ou des fenêtres contextuelles) lorsque les utilisateurs du site Web peuvent avoir une décision à prendre ou se poser une question concernant la protection de la vie privée. » De plus, toujours selon le Commissariat à la vie privée du Canada, l'information contenue dans la politique de confidentialité devrait être accessible de diverses manières, par exemple, en personne, dans des publications écrites, par téléphone, en plus du site Web de l'organisation. Cela est cohérent avec le principe de neutralité technologique. D'ailleurs, le premier alinéa de l'article 6 pourrait être reformulé ainsi : « Une politique de confidentialité et un avis de modification doivent être rédigés en termes simples et clairs, publiés dans une section dédiée à cette politique sur le site Internet de l'organisme public et diffusés par tout moyen propre à atteindre les personnes concernées. »
Il est pertinent d'utiliser l'approche téléologique afin de questionner la finalité de cet article où le législateur souhaite que les citoyens soient avisés de la politique de confidentialité et de l'avis de modification. En ce sens, il est nécessaire que l'information soit disponible facilement et que son accessibilité soit garantie. Le projet de règlement implique, à l'article 6, que ces informations soient « publiées dans une section dédiée à cette politique sur le site internet ». À mes yeux, cette publication n'est pas suffisante, à elle seule, pour répondre au but du législateur, malgré l'obligation fondamentale de se renseigner qui	En principe, une publication sur le site Internet de l'organisme représente la méthode de publicisation la plus courante, simple et favorable à l'approche par couche, permettant à l'individu d'accéder au niveau de détail souhaité (transparence). En revanche, ce choix représente une contravention au principe de neutralité technologique consacré par la *Lccjti* en priorisant un mode de diffusion par Internet. Cela pose problème dans la mesure où certaines personnes peuvent fournir des renseignements personnels par moyen technologique sans avoir recours à Internet (par exemple, par l'entremise d'un poste

incombe aux citoyens et qui est réitérée dans la décision Banque de Montréal c. Bail Ltée (p. 587, 1992). Toutefois, à mes yeux, l'analyse de l'article 6 du projet de règlement est impossible, sans la considération de l'article 7, qui implique que l'avis de modification et la politique de confidentialité doivent « être portés à l'attention de la personne concernée par ces renseignements » permettant de répondre au but du législateur. Cependant, par souci de neutralité technologique, le projet de règlement n'impose pas de format spécifique. La situation est similaire au niveau du secteur privé, qui doit « diffuser par tout moyen propre à atteindre les personnes concernées » ces informations, en vertu de l'article 107 de la *Loi 25* modifiant l'article 8.2 de la *Loi dans le secteur privé*. Or, l'interprétation peut impliquer de nombreux moyens d'avertir les personnes, incluant un courriel, une bannière, ou une fenêtre surgissante. Est-ce que tous ces formats sont valides au sens du règlement ? Il sera important de surveiller l'application concrète de cet article afin d'assurer l'accessibilité de l'information aux citoyens.	fixe, par SMS). Cela pose un enjeu au niveau du principe de démontrabilité, en vertu duquel l'organisme doit être en mesure de démontrer la validité du consentement obtenu (par. 22). De plus, l'exigence ne saura pas survivre à l'épreuve du temps, notamment avec l'avènement de nouvelles technologies (par exemple, la réalité augmentée/virtuelle). Il aurait été souhaitable de laisser place à l'équivalence fonctionnelle, en prévoyant plutôt la finalité à atteindre (accessibilité, publicisation), qui peut ultimement se faire par Internet, par papier, par panneau, ou par téléphone (service automatisé) de façon à rendre la politique accessible et publique. Les réseaux sociaux permettent aussi un mode de diffusion efficace. Enfin, le RGPD propose l'idée la plus intéressante, soit l'utilisation d'icônes standardisé pour fournir l'information. Bien que la régulation européenne apporte peu de précisions à cet égard, il serait pertinent de concevoir certaines mentions par l'entremise d'icônes (tel que l'icône du cadenas qui signifie une connexion sécure par certificat de chiffrement). Ces icônes peuvent être standardisés par une ligne directrice de la CAI, assurant l'harmonisation. Encore là, seule une formulation conforme à la neutralité technologique aurait permis ce genre d'innovation pour mieux informer l'individu. *La politique et l'avis de modification doivent être diffusé par tout moyen jugé adéquat par le comité sur l'accès à l'information […].*
La méthode de publication de la politique de confidentialité et de l'avis de modification présente un enjeu de neutralité technologique. Les personnes qui se font aider pour accomplir les démarches en ligne, notamment les personnes qui ne sont pas à l'aise avec la technologie informatique et les personnes qui souffrent d'un handicap, ne seront sans doute pas informées de la politique de confidentialité en place, ni de sa modification. Pourtant, les organismes doivent faire parvenir la politique par tout « moyen propre à atteindre les personnes concernées » selon la base légale. Cette même disposition apparaît dans la Loi sur le secteur privé. Ce point ne faisant pas l'objet d'un règlement, on peut penser qu'il s'appliquera tel quel pour le secteur privé. Cette précaution est pourtant prise à l'extérieur du Québec, pour l'ensemble des provinces, car la Loi fédérale (LPRPDÉ) s'applique (à l'exception de l'Alberta et de la Colombie Britannique qui ont leur propre loi en la matière). Ainsi l'article 6 ne nous semble pas conforme, il nie la notion de « tout moyen propre à atteindre les personnes concernées » et va à l'encontre de la majorité des pratiques hors Québec. Proposition : « Une politique de confidentialité et un avis de modification doivent être publiés dans une section	En se fiant aux informations disponibles sur le site de la *Loi sur l'accès*, la neutralité technologique constitue un désintéressement du cadre technologique où aucune technologie n'est avantagée au détriment d'une autre. Ainsi, sous réserve d'une précision expresse par la loi, toute personne peut utiliser le moyen technologique qu'elle désire. En l'espèce, l'article 6 précise qu'une politique de confidentialité et un avis de modification « doivent être publiés dans une section dédiée à cette politique **sur le site Internet** de l'organisme public ». La mention d'une publication sur un site Internet constitue, selon moi, un manque de neutralité technologique. Quand est-il des applications mobiles ? En gardant l'objectif du législateur en tête, il me semble incohérent de publier uniquement une politique de confidentialité et ses avis de modifications sur un site Internet. En effet, cela va à l'encontre du principe d'accessibilité de l'information. D'une part, il me semble peu probable qu'une personne prenne le temps d'aller observer, sur le site Internet d'une application qu'elle possède uniquement sur son téléphone (temps et manque de simplicité), une politique de confidentialité. D'autre part, l'aspect de notification lors d'une publication d'un avis de

dédiée à cette politique sur le site Internet de l'organisme public, et transmise aux personnes concernées par tout moyen propre à les atteindre. La plus récente version antérieure de la politique et l'avis de modification correspondant, le cas échéant, doivent aussi être publiés dans la section dédiée à la politique de confidentialité. Ils doivent être transmis aux personnes concernées par tout moyen propre à les atteindre. L'organisme public doit veiller à ce que cette version antérieure de la politique ne soit pas confondue avec la version en vigueur. »	modification manque de clarté. Prenons le cas d'une application mobile : devrions-nous avoir une notification directement sur l'application ou le site Internet ? L'article 3.2 de la *Loi sur le secteur privé* mentionne également de faire une publication sur le site Internet, **mais** elle ajoute qu'en cas où l'entreprise n'a pas de site, elle peut le faire par tout autre moyen approprié. Selon moi, on retrouve le même problème par rapport à la publication priorisée sur les sites Internet. Somme toute, cet article devrait comporter une mention « publication par tout moyen facilement accessible pour l'utilisateur » ainsi qu'une précision quant au mode de notification lors de la publication d'un avis de modification.

ANNEXE 1 – QUESTIONNAIRE D'ÉVALUATION

Politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique[2]

Commentaires dans le cadre du cours DRT871 et BIM717

1. QUESTIONS GÉNÉRALES	
1.1	Quelle évaluation générale faites-vous du projet de règlement ? *Donner votre évaluation sur une échelle de 1 à 5 (soit 1 très négative à 5 très positif) en justifiant par des explications (250 mots maximum).*
1.2	Le projet de règlement vous parait-il valide du point de vue juridique ? Les orientations qu'il donne sont-elles cohérentes entre elles ? *Donner votre évaluation sur une échelle de 1 à 5 (soit 1 pas du tout conforme à loi à 5 parfaitement conforme à la loi) en justifiant par des explications appuyées par des articles de loi (250 mots maximum).*
1.3	Le projet de règlement a-t-il une portée adéquate compte tenu de son objectif ? Est-il complet ? *Donner votre évaluation sur une échelle de 1 à 5 (soit 1 très incomplet à 5 très complet) en justifiant par des propositions d'ajout avec suffisamment de détails (250 mots maximum).*
1.4	Pensez-vous que ce projet de règlement peut être appliqué concrètement et qu'il est réaliste ? Anticipez-vous des conséquences négatives découlant des orientations présentées, et, si oui, lesquelles ? *Donner votre évaluation sur une échelle de 1 à 5 (soit 1 très difficile à 5 très facile) en justifiant par des exemples concrets (250 mots maximum).*
1.5	Le format du projet de règlement est-il adapté et en facilite-t-il la consultation ? Le texte est-il suffisamment clair ? *Donner votre évaluation sur une échelle de 1 à 5 (soit 1 pas clair du tout à 5 très clair) en justifiant par des exemples concrets (250 mots maximum).*

[2] Projet de règlement Gazette No. 28 du 12-07-2023, page : 3246, en ligne : https://www.publicationsduquebec.gouv.qc.ca/fileadmin/gazette/pdf_encrypte/lois_reglements/2023F/80218.pdf

2. QUESTIONS SPÉCIFIQUES	
2.1	Article 1 : Que pensez-vous du champ d'application du projet de règlement ? Est-ce que tous les organismes publics ainsi que le secteur privé devraient y être assujettis ? *Fournir des explications avec suffisamment de détails en proposant une version modifiée de l'article 1, le cas échéant (300 mots maximum).*
2.2	Article 2 : Que pensez-vous du contenu que devrait contenir une politique de confidentialité ? Est-ce trop ou pas assez détaillé ? *Fournir des commentaires en faisant notamment référence aux travaux de la Commission d'accès à l'information du Québec, le Commissariat à la protection de la vie privée du Canada ainsi que toute autre disposition législative ou lignes directrices d'une autorité de contrôle, et en proposant une version modifiée de l'article 2, le cas échéant (300 mots maximum).*
2.3	Article 3 : Que pensez-vous de la collecte commune de renseignements personnels par plusieurs organismes publics ? Qui est alors responsable et détient ces renseignements (notamment en matière de respect des droits des individus, etc.) ? *Fournir des commentaires en faisant référence aux principes de la Loi sur l'accès, identifier de possibles incohérences ou contradictions, et proposer une version modifiée de l'article 3, le cas échéant (300 mots maximum).*
2.4	Article 4 : Que pensez-vous de l'obligation d'un avis de modification pour toute modification (significative ou non) à une politique de confidentialité dans un délai de 15 jours ? Avez-vous des commentaires concernant le format ou les exigences y étant reliés ? *Fournir des commentaires en faisant référence à d'autres exemples (y compris dans le secteur privé et en-dehors du Québec) en proposant une version modifiée de l'article 4, le cas échéant (300 mots maximum).*
2.5	Article 6 : Que pensez-vous de la méthode de publicisation d'une politique de confidentialité et de l'avis de modification ? *Fournir des commentaires en faisant référence à d'autres exemples (y compris dans le secteur privé et en-dehors du Québec) en proposant une version modifiée de l'article 6, le cas échéant (300 mots maximum).*

CONSENTEMENT

☐ [OBLIGATOIRE] Je certifie avoir respecté la déclaration d'intégrité et engagement applicable au travail de session (qui doit être signée et transmise séparément à l'enseignant au surplus).

☐ [FACULTATIF] J'accepte que les réponses données aux questions dans le cadre du présent travail soient rendues publiquement accessibles et transmises dans leur intégralité au *Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité* dans l'objectif de commenter et améliorer le projet de règlement Gazette No. 28 du 12-07-2023, page : 3246.

- Les réponses seront transmises dans un rapport agrégé et dépersonnalisé qui contiendra les réponses d'au moins cinq (5) étudiant/es et sans aucun nom et prénom des auteur/es de ces commentaires. Autrement dit, ce rapport agrégé parlera génériquement des commentaires obtenus dans le cadre de l'École d'été DRT871 et BIM717 de l'année 2023 sans y mentionner les noms et prénoms des individus ayant écrit des commentaires et/ou ayant participé au cours. Veuillez toutefois noter que vous pourriez être identifié indirectement en relation avec les opinions exprimées dans vos réponses.

- L'enseignant se réserve le droit de ne pas rendre publique et/ou transmettre vos réponses, ou d'y corriger des erreurs de nature purement orthographique (sans en affecter le contenu) avant publication/transmission.

- **Il n'y a aucune conséquence liée au fait de ne pas consentir, y compris concernant votre résultat final à cette évaluation.**

Nom et prénom :

Date :

Signature :

ANNEXE 2 – PROJET DE RÈGLEMENT

2. Le présent règlement entre en vigueur à la date de sa publication à la *Gazette officielle du Québec*.

80254

Projet de règlement

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1)

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (2021, chapitre 25)

Politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique

Avis est donné par les présentes, conformément aux articles 10 et 11 de la Loi sur les règlements (chapitre R-18.1), que le projet de règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique, dont le texte apparaît ci-dessous, pourra être édicté par le gouvernement à l'expiration d'un délai de 45 jours à compter de la présente publication.

La Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (2021, chapitre 25), sanctionnée le 22 septembre 2021, introduit dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) l'article 63.4. En vertu de cette disposition, un organisme public qui recueille par un moyen technologique des renseignements personnels doit publier sur son site Internet et diffuser par tout moyen propre à atteindre les personnes concernées une politique de confidentialité rédigée en termes simples et clairs. Il doit en faire de même pour l'avis dont toute modification à cette politique doit faire l'objet.

Ce projet de règlement vise à déterminer le contenu et les modalités de cette politique et de cet avis.

Pour les citoyens, ce projet de règlement permet d'harmoniser le contenu des politiques de confidentialité des organismes publics, auxquelles ces derniers auront accès, notamment lors d'une collecte de renseignements personnels par un moyen technologique faite par un organisme public. Ces politiques leur permettent également d'obtenir les informations nécessaires afin qu'ils puissent comprendre leurs droits et de quelle façon leurs renseignements personnels sont recueillis et utilisés.

Ce projet de règlement n'a pas de conséquence sur les entreprises, en particulier les PME.

Des renseignements additionnels concernant ce projet de règlement peuvent être obtenus en s'adressant à monsieur Christian Duquette, avocat, Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité, ministère du Conseil exécutif, 875, Grande Allée Est, bureau 3.263, Québec (Québec) G1R 4Y8; téléphone: 418 528-8024, poste 5140; courriel: christian.duquette@mce.gouv.qc.ca.

Toute personne intéressée ayant des commentaires à formuler au sujet de ce projet de règlement est priée de les faire parvenir par écrit, avant l'expiration du délai de 45 jours mentionné ci-dessus, à madame Julie Samuël, directrice de l'accès à l'information et de la protection des renseignements personnels au Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité, ministère du Conseil exécutif, 875 Grande Allée Est, bureau 3.265, Québec (Québec) G1R 4Y8; courriel: daiprp@mce.gouv.qc.ca.

Le ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels,
JEAN-FRANÇOIS ROBERGE

Règlement sur les politiques de confidentialité des organismes publics recueillant des renseignements personnels par un moyen technologique

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1, a. 63.4, 2e al. et a. 155, 1er al., par. 6°)

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (2021, chapitre 25, a. 15)

SECTION I
CHAMP D'APPLICATION ET DÉFINITION

1. Le présent règlement s'applique à tout organisme public visé à l'article 3 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1).

Il s'applique également aux ordres professionnels, dans la mesure prévue par le Code des professions (chapitre C-26).

Pour l'application du présent règlement, l'expression « organisme public » comprend un ordre professionnel.

SECTION II
POLITIQUE DE CONFIDENTIALITÉ

2. Une politique de confidentialité visée à l'article 63.4 de la Loi doit minimalement contenir :

1° le nom de l'organisme public qui recueille les renseignements personnels et, dans le cas où les renseignements sont recueillis par un tiers au nom de l'organisme public, le nom de ce tiers;

2° une description des renseignements personnels recueillis;

3° les fins auxquelles les renseignements personnels sont recueillis;

4° les catégories de personnes qui, au sein de l'organisme public, ont accès aux renseignements personnels;

5° les moyens par lesquels les renseignements personnels sont recueillis;

6° le cas échéant, une description des mesures pouvant être prises afin de refuser la collecte des renseignements personnels et les conséquences possibles en résultant;

7° le cas échéant, une mention relative aux moyens technologiques disponibles pour que la personne concernée par les renseignements personnels puisse consulter ou rectifier ces renseignements;

8° une mention relative aux droits d'accès et de rectification prévus par la Loi, de même que le nom du responsable de la protection des renseignements personnels de l'organisme public et les coordonnées permettant de communiquer avec lui;

9° le cas échéant, le nom des tiers ou des catégories de tiers à qui il est nécessaire de communiquer des renseignements personnels aux fins visées au paragraphe 3°, en précisant ces renseignements ou les catégories de renseignements et ces fins;

10° le cas échéant, une mention quant à la possibilité que les renseignements personnels soient communiqués à l'extérieur du Québec;

11° une brève description des mesures prises pour assurer la confidentialité et la sécurité des renseignements personnels;

12° une mention du droit de la personne concernée par les renseignements personnels de se prévaloir du processus de traitement des plaintes relatives à la protection des renseignements personnels prévu dans les règles de gouvernance de l'organisme public à l'égard des renseignements personnels publiés en vertu de l'article 63.3 de la Loi;

13° les coordonnées de la personne, de l'organisme concerné ou d'une unité administrative de ce dernier à qui toute question relative à cette politique de confidentialité peut être soumise;

14° la date de son entrée en vigueur et la date de sa plus récente mise à jour, le cas échéant.

3. Une politique de confidentialité peut être commune à plusieurs organismes publics dans la mesure où ils recueillent en commun des renseignements personnels.

Elle peut également être commune à plusieurs organismes publics dans la mesure où un organisme public recueille des renseignements personnels au nom des autres organismes publics.

SECTION III
AVIS DE MODIFICATION

4. Une politique de confidentialité ne peut être modifiée avant l'expiration d'un délai de 15 jours à compter de la date de publication d'un avis de modification de cette politique ou, le cas échéant, avant l'expiration d'un délai plus court mentionné dans cet avis de modification. Cet avis doit:

1° indiquer la date de sa publication;

2° indiquer l'objet général des modifications apportées à la politique de confidentialité, lesquelles doivent être précisées dans une section dédiée à cette politique sur le site Internet de l'organisme public;

3° indiquer la date de l'entrée en vigueur des modifications;

4° si l'avis mentionne un délai plus court que le délai de 15 jours, indiquer les motifs pour lesquels la politique doit être modifiée dans ce délai plus court.

SECTION IV
DISPOSITIONS COMMUNES À UNE POLITIQUE DE CONFIDENTIALITÉ ET À UN AVIS DE MODIFICATION

5. Une politique de confidentialité doit, avant d'être publiée, faire l'objet d'une consultation auprès du comité sur l'accès à l'information et la protection des renseignements personnels visé à l'article 8.1 de la Loi.

Il en est de même de tout avis de modification concernant une modification significative à une politique.

6. Une politique de confidentialité et un avis de modification doivent être publiés dans une section dédiée à cette politique sur le site Internet de l'organisme public.

La plus récente version antérieure de la politique et l'avis de modification correspondant, le cas échéant, doivent aussi être publiés dans cette section. L'organisme public doit veiller à ce que cette version antérieure de la politique ne soit pas confondue avec la version en vigueur.

7. Lors de la collecte de renseignements personnels par un moyen technologique, la politique de confidentialité concernant ces renseignements personnels et, le cas échéant, l'avis de modification de cette politique doivent être portés à l'attention de la personne concernée par ces renseignements.

SECTION V
DISPOSITION FINALE

8. Le présent règlement entre en vigueur le 1er janvier 2024.

80218