



Présentation détaillée

Montréal, le 8 septembre 2022

Enjeux sur le portefeuille d'identité numérique québécois

À l'attention des députés et des ministres responsables du portefeuille numérique, ainsi qu'aux candidats aux élections du Québec 2022.

Objet :

1. Que les futurs élus et candidats soient informés des pratiques des institutions bancaires actuelles et à venir qui portent atteinte aux droits fondamentaux, au respect de la vie privée et contreviennent aux exigences légales de protection des renseignements personnels (PRP) afin qu'ils puissent mettre en œuvre les actions nécessaires pour faire cesser ces pratiques.
2. Qu'ils prennent l'engagement, dans le cadre de la transformation numérique de l'état québécois y compris le projet de portefeuille d'identité numérique, d'exercer une vigilance constante pour :
 - Prévenir toute atteinte au respect de ces droits, y compris le droit fondamental à la liberté, à l'autonomie des citoyens ;
 - Que les citoyens demeurent souverains de leurs données personnelles ;
 - Que toute politique de confidentialité devienne un contrat réciproque.

Les faits

Des milliers de citoyens ont été confrontés, depuis février 2022, à la mise en place d'une nouvelle politique de confidentialité chez Desjardins et par des banques. Des milliers de membres chez Desjardins sont très préoccupés par le manque de transparence et d'honnêteté de la demande de

consentement à laquelle ils furent obligés de consentir et par le fait qu'il est maintenant impossible de le retirer.

De nombreuses personnes ont déjà porté plainte à l'Autorité des marchés financiers où l'équipe de consentement Desjardins y réfère ses clients pour porter plainte. L'AMF répond pourtant qu'elle ne traite pas les affaires liées au consentement ni de politique de confidentialité.

Plaintes formulées auprès de la Vice-présidence à la conformité de Desjardins, à la Commission d'accès à l'information et au Commissariat à la protection de la vie privée du Canada, de Desjardins et de certaines banques

Des plaintes ont été envoyées par des centaines de membres chez Desjardins et chez certaines banques. Non seulement les réponses de l'équipe du consentement de Desjardins furent insatisfaisantes au regard de l'importance des enjeux, mais nous avons constaté que les conseillers ne sont pas formés pour répondre aux clients dès lors qu'il s'agit de nos lois en vigueur sur la protection des renseignements personnels (ci-après PRP) et plus particulièrement du consentement¹.

La modernisation des lois

Par ailleurs, de 2019 à 2021, les projets de lois n°14 et 95 et 6, ont été sanctionnés à l'Assemblée nationale du Québec. Ils encadrent la transformation numérique de l'administration publique, y compris le projet de portefeuille d'identité numérique². C'est en prétextant devoir répondre à ces nouvelles obligations légales que les institutions bancaires ont mis à jour leur politique générale de confidentialité pour forcer le consentement des clients à utiliser les services en ligne et à recueillir et utiliser des données personnelles de nature sensible.

Ces projets de lois, soumis par le ministre Éric Caire, créent un régime parallèle de PRP ignorant le caractère prépondérant des lois québécoises à cet égard. Elles s'inscrivent en faux quant à l'esprit même du projet de loi n° 64 modifiant les lois québécoises sur la PRP qui rehausse la protection de nos données dans un contexte numérique accru³ (voir le [Mémoire de la CAI](#)).⁴

N'est-il pas discutable et incohérent que le ministre Caire, qui est tout à la fois responsable des lois sur la transformation numérique et des lois sur la PRP vise des objectifs contradictoires ?⁵

¹ [Loi sur l'accès aux documents et sur la protection des renseignements personnels](#)

[Loi sur la protection des renseignements personnels dans le secteur privé – Projet de loi 64 Loi modernisant la Loi sur la protection des renseignements personnels et les documents électroniques \(LPRPDE\)](#)

² [Projet de loi n° 14 - Loi favorisant la transformation numérique de l'administration publique. \(2019, chapitre 17\) Sanctionné le 10 octobre 2019. - \[Projet de loi n° 95 - Loi modifiant la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement et d'autres dispositions législatives. \\(2021, chapitre 22\\) Sanctionné 10 juin 2021 et \\[Projet de loi n° 6 Loi édictant la Loi sur le ministère de la cybersécurité et du numérique et modifiant d'autres dispositions \\\(Chapitre M-17.1.1\\\). Sanctionné le 3 décembre 2021.\\]\\(#\\)\]\(#\)](#)

³ [Projet de loi n° 64 Loi modernisant des dispositions législatives en matière de protection des renseignements personnels \(2021, chapitre 25\) Sanctionné le 22 septembre 2021.](#)

⁴ [Mémoire de la CAI](#) déposés lors des travaux parlementaires sur le Projet de loi 94. 21 mai 2021.

⁵ M. Éric Caire est Ministre de la Cybersécurité et du Numérique depuis le 1 janvier 2022 et Ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels depuis le 21 janvier 2021

De cet état de fait, associé à l'approche de contrainte du consentement de Desjardins et à la tendance des institutions financières, de grandes inquiétudes ont émergé.

Le contexte dans lequel le Mouvement Desjardins prétend répondre des lois

Pour vous mettre en contexte, Desjardins présente à la clientèle qui accède à son compte en ligne, une interface pour adhérer, sans préavis, à la nouvelle Politique de confidentialité. Il plaide qu'il a choisi cette manière pour une meilleure efficacité de communication avec tous ses membres et pour plus de transparence.

Le contrat de confidentialité prévoit la cueillette d'une surenchère de renseignements personnels que Desjardins peut ou voudra détenir afin de livrer les produits et services utilisés par la clientèle. Également, cette nouvelle politique lui permet, répond-il, de respecter son nouveau cadre légal au regard de la modernisation des lois et du portefeuille d'identité numérique du gouvernement du Québec. Ce contrat unilatéral de confidentialité prévoit également que Desjardins pourrait obtenir d'un tiers des renseignements personnels leur permettant d'offrir des produits et services mieux personnalisés.

Le client a-t-il le choix ?

En ce qui a trait aux banques, le client, comme chez Desjardins, n'a aucun choix concernant ses renseignements personnels. La banque envoie simplement une lettre l'avisant des nouvelles politiques de confidentialité.

Quant au Mouvement Desjardins qui a souhaité faire montre de plus de transparence, il affirme que nous avons toujours le choix. Or le seul choix immédiatement visible présenté par l'interface d'AccèsD, pour poursuivre l'accès au compte en ligne est celui de consentir à la nouvelle politique ou de pouvoir reporter une seule fois notre décision forcée. Lorsque le client reporte sa décision, il est tout de suite avisé que son consentement sera obligatoire la prochaine fois qu'il voudra accéder à son compte en ligne. **Ce qui ne relève pas, comme stipulé par la loi, d'un consentement libre et constitue ni plus ni moins une extorsion du consentement de ses membres.**

Le contrat sur la confidentialité est donc rédigé unilatéralement, et de toute évidence, il est surtout à l'avantage de Desjardins puisque le client n'a pas son mot à dire.

La conséquence de ses choix

Depuis février, le refus par la clientèle de consentir à la politique de confidentialité de Desjardins a pour conséquence immédiate et directe de ne plus pouvoir accéder au compte en ligne AccèsD pour effectuer ses transactions financières. Les membres qui n'adhèrent pas ont ultérieurement appris qu'ils pouvaient toutefois se déplacer physiquement à la Caisse pour faire leurs opérations. Cette conséquence contrevient à la loi qui énonce :

On ne peut priver d'un service une personne sous le prétexte qu'elle ne désire pas fournir des renseignements privés.

Plusieurs citoyens nous ont informés qu'ils n'ont maintenant plus accès à leur compte en ligne, n'ayant pas donné leur consentement à cette nouvelle politique. Cette réalité s'est produite avec d'autres institutions que Desjardins. Des agents de Desjardins ont indiqué qu'il est prévu dans un

avenir rapproché de ne plus offrir la possibilité de faire des transactions en personne dans les caisses, migrant les services en totalité vers le numérique. Les banques sont en train d'emboîter le pas.

D'autres citoyens nous ont aussi informés qu'ils ont été dans l'obligation de fournir leur consentement pour pouvoir continuer de faire des transactions bancaires en ligne, leur système d'opérations étant structuré autour de transactions électroniques. Ils se demandent aujourd'hui comment retirer leur consentement puisqu'ils y furent forcés. Desjardins refuse catégoriquement d'effectuer le retrait du consentement des membres mécontents.

De plus, un consentement à une politique générale permettant à Desjardins de recueillir, utiliser ou communiquer des renseignements personnels est contraire aux principes et objectifs de la Loi sur le secteur privé.

Nous soumettons à votre attention que, sur son site, le mouvement recommande l'usage d'AccèsD tout en bloquant ceux qui refusent les nouvelles politiques de confidentialité. Comment prétendre que son client a le choix de refuser de poursuivre ses transactions sur AccèsD ? Comment prétendre répondre à ses obligations légales alors que le Mouvement Desjardins transgresse la Loi sur la protection des renseignements personnels dans le secteur privé?

Desjardins transgresse la loi en ce qui concerne les critères d'un consentement valide, le droit de retirer son consentement et l'obligation d'informer les membres de façon spécifique et non pas générale comme le fait Desjardins lorsqu'il recueille, utilise et communique des renseignements personnels.

Les lois bafouées

Rappel de l'encadrement légal du respect de la vie privée et des lois sur la PRP au Québec et au gouvernement fédéral

Les lois québécoises sur l'accès à l'information reposent sur le droit à l'information et à la vie privée consacrées dans la Charte des droits et libertés de la personne. Elles ont un statut particulier et sont prépondérantes aux autres lois du Québec.

Les activités de Desjardins à l'extérieur du Québec sont régies par la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).⁶

Les lois de PRP reposent sur le principe fondamental que toute personne a un droit de regard sur les renseignements qui la concernent et qui peuvent être colligés, rendus accessibles, utilisés, communiqués, conservés et détruits par un organisme public ou une entreprise privée. Ces activités représentent les moments clés du cycle de vie des renseignements personnels.

Le consentement extorqué par Desjardins et la privation de biens et services

L'article 14 de la Loi sur la protection des renseignements personnels dans le secteur privé mentionne que *le consentement 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*. Et ce

⁶ [Loi sur la protection des renseignements personnels et les documents électroniques \(LPRPDE\)](#). L.C. 2000, ch. 5.

consentement ne vaut *que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé.*

Or ici, on oblige la clientèle à donner son consentement à la politique dans son intégralité, sous peine de lui retirer l'accès au compte en ligne pour effectuer de ses transactions financières avec les méthodes courantes et habituelles, donc l'accès à son argent par ses méthodes habituelles de paiements.

L'article 9 de cette même Loi précise que *nul* (il faut comprendre ici les entreprises) *ne peut refuser d'acquiescer à une demande de bien ou de service en raison du refus de la personne qui formule la demande, de lui fournir un renseignement personnel.*⁷

Le bien étant l'accès à l'argent dans le compte pour couvrir les besoins essentiels et entrepreneuriaux. Desjardins se donne le droit de couper cet accès aux biens en interrompant le service AccèsD. Desjardins contraint le membre à renoncer à sa liberté de choix et à son pouvoir d'achat, grâce au service AccèsD, tant personnel que professionnel.

Cette contrainte soudaine soulève un enjeu majeur qui devrait non seulement interpeller la Commission d'accès à l'information, le Commissariat à la protection de la vie privée au Canada⁸, mais aussi la Commission des droits de la personne et l'Office de la protection du consommateur, Option Consommateur, les Associations coopératives d'économie familiale (ACEF) et d'autres organismes de défense des droits des consommateurs.

Respect de la Charte des droits et libertés

L'article 5 de la Charte des droits et libertés de la personne du Québec énonce que toute personne a droit au respect de sa vie privée. Selon l'article 6 : « *Toute personne a droit à la jouissance paisible et à la libre disposition de ses biens, sauf dans la mesure prévue par la loi* ».

Desjardins devra démontrer que sa politique n'est pas discriminatoire, tel que le stipule **l'article 10 de la Charte**, d'autant plus que le Mouvement Desjardins semble prévoir, dans un futur proche, que ses membres fassent uniquement leur transaction en ligne.

Par exemple, une personne qui n'est pas en mesure de se déplacer pour aller au guichet de la caisse (mobilité réduite, handicap, etc.) et qui a refusé de consentir à fournir ses données privées, peut-elle continuer de bénéficier des transactions en ligne du service AccèsD ? Un entrepreneur qui a été encouragé par l'environnement numérique à héberger son système de transactions en ligne peut-il continuer de l'utiliser sans devoir fournir des renseignements qu'il juge abusif ?

Pourquoi la nature des renseignements personnels exigés relève-t-elle de la seule décision des institutions bancaires sans que le client ait son mot à dire dans ce contrat ? Un contrat doit être conclu de manière consensuelle entre les parties.

⁷ Loi sur la protection des renseignements personnels dans le secteur privé: article 14. Le consentement 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. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. Voir également l'article 8 de cette Loi sur la protection des renseignements personnels dans le secteur privé et l'article 107 du Projet de Loi n° 64.

Un consentement qui n'est pas donné conformément au premier alinéa est sans effet.

⁸ Des plaintes ont été déposées le 29 août dernier à commissaire fédéral et à la CAI.

L'enjeu: une inversion insidieuse des principes et objectifs de la Loi sur la protection des renseignements personnels dans le secteur privé

Plusieurs échanges que nous avons eus avec des citoyens relativement à cette situation, confirment une inversion de l'esprit de la loi. De leur côté, les conseillers contactés au Mouvement Desjardins, nous ont indiqué que cette nouvelle façon de faire est rendue nécessaire en raison des « *nouvelles dispositions légales de protection des renseignements personnels* ».

Comme mentionné précédemment, les articles 9 et 14 protègent le citoyen contre l'abus et l'extorsion du consentement et une collecte abusive. Si Desjardins et les autres institutions bancaires détenaient déjà un portefeuille de données privées sur leurs clients, la loi les oblige aujourd'hui à faire preuve de plus de transparence quant à la gestion des renseignements, soutirés au fil du temps, souvent à leur insu.

Aujourd'hui, le client ne semble pas avoir son mot à dire sur les données que les institutions possèdent à son sujet. Et cela pose un grave problème de légitimité concernant le droit de posséder des renseignements recueillis antérieurement, basés sur un consentement nébuleux.

Dans le contexte de la modernisation des lois, le gouvernement est-il en train de cautionner, grâce au secteur privé, un environnement bionumérique où toute entreprise peut détenir une quantité non justifiée de données privées sur ses clients et les utiliser comme bon lui semble ? Est-il normal que les clients doivent renoncer à leurs droits fondamentaux (vie privée, etc.) en échange d'un service vital, comme celui d'accéder à ses avoirs dûment gagnés ?

Pour mieux comprendre l'esprit des nouvelles modifications légales, notamment celles du projet de loi 64, Loi modernisant des dispositions législatives en matière de PRP, vous pouvez consulter le [Mémoire](#) déposé par la ministre Sonia Lebel.

Pourquoi certains acceptent et d'autres refusent le consentement ?

Certains membres de Desjardins ressentent un malaise et perçoivent que la demande de consentement n'est pas transparente, qu'elle n'est pas à leur avantage, qu'ils perdent quelque chose.

L'utilisation de la politique de consentement est insidieuse dans sa manière de contraindre le membre à renoncer à ses droits fondamentaux, à défaut de quoi il sera privé du service AccèsD. Pour accéder à nos biens essentiels, notamment à l'accès à notre argent en ligne, nous devons renoncer à nos droits fondamentaux.

Il s'agit ici d'une inversion insidieuse des objectifs visés par la responsabilité qu'a une entreprise de produire et de diffuser une politique de PRP. Cette façon de faire sournoise est immorale et sape la confiance du membre, malgré lui. De plus, elle est contraire à l'esprit de la loi.

Bien que l'engagement de Desjardins à l'égard de la PRP paraisse de prime abord rassurant pour les membres, Desjardins inverse l'esprit de la politique. Ce qui explique, de ce fait, pourquoi le membre a l'intuition d'être floué.

Changer de banque ?

On nous informe aussi que toutes les institutions financières iront dans le même sens. Pire, elles prennent le consentement aux nouvelles politiques de confidentialité pour acquis. Est-ce que tous les citoyens seront touchés de la sorte par ces nouvelles politiques intrusives ?

Or, cette pratique ouvre la porte à toutes les autres entreprises privées et commerciales. Elles seront à leur tour tentées d'extorquer, auprès de milliers de clients, un consentement ni éclairé et ni libre.

Ce bar ouvert se fait au nom de la sécurité, alors même que les consommateurs doivent renoncer à être propriétaires de leurs données privées. Et que rien, ni personne ne peut assurer à 100% la sécurité des données.

Futurs élus et candidats, nous vous prions de porter rapidement à l'attention du gouvernement cette entorse à la loi et de la corriger impérativement. Comme futur élu, il est impératif que vous conscientisiez ces enjeux.

Qui est le chien de garde des citoyens au gouvernement ?

Le gouvernement ne semble pas s'offusquer de voir les institutions bancaires contrevenir à la Loi sur la protection des renseignements personnels dans le secteur privé, qui a préséance sur toutes les autres lois. Elles font pourtant entorse aux articles 9 et 14 à cette Loi et, de ce fait, devraient être imputables. Ne pas en convenir ni sévir créera un grave précédent ouvrant la porte à toute entreprise de faire des demandes abusives de renseignements personnels, tels les commerces.

Avec autant de données en circulation dans les entreprises et commerces, le profilage sera facilité. Le gouvernement a déjà en tête d'outrepasser l'usage administratif des données personnelles de chaque citoyen. Le profilage sera ni plus ni moins l'instauration d'un régime de surveillance à crédit social.

Il nous apparaît inacceptable que le gouvernement – qui recueillera les mêmes données pour la création du portefeuille numérique et qui se présente en gardien de nos identités numériques – puisse laisser l'impression que les institutions bancaires et toutes entreprises privées pourraient exiger les mêmes clés d'identification, sachant qu'elles y auront accès via le portefeuille numérique.

La cybersécurité ne garantit pas la protection des données personnelles

La sécurité de l'information y compris la cybersécurité est une notion distincte de la PRP et elle doit être considérée comme un des moyens d'assurer le respect de nos droits. Elle n'est donc pas garante de la PRP au sens des lois qui s'appliquent.⁹

Lors de ses communications publiques ainsi que dans les lois dont il est responsable et qui régissent les activités de la transformation numérique, le ministre Caire confond la cybersécurité et le respect des lois de PRP.

⁹ Voir à ce sujet le [Guide de l'infonuagique. Architecture d'entreprise gouvernementale 3.0. Volume 2 – Considérations juridiques et de protection des renseignements personnels](#). Secrétariat du conseil du trésor. Novembre 2014.

Centraliser, la porte ouverte au crédit social

Sachant que la sécurité des données ne peut être garantie à 100% par aucune entité publique et encore moins privée, plus les citoyens fourniront de renseignements personnels centralisés, plus leurs données seront fragilisées.

La sécurité ne peut donc pas être invoquée par les institutions bancaires ni par le ministre de la cybersécurité et du numérique comme justification principale à une demande abusive de données personnelles. Au contraire, en cas de fraude, davantage de nos renseignements seront à risque. Plusieurs incidents de sécurité sont rapportés régulièrement¹⁰. Tout le monde se souvient des incidents majeurs de sécurité chez Desjardins entre 2017 et 2019 qui a mis en péril des données d'identité et financières de 9,7 millions de personnes au Canada et à l'étranger, dont près de 7 millions de Québécois, ont été victimes de ce vol de données¹¹. La CAI et le Commissaire fédéral au respect de la vie privée ont fait enquête et formulé une série de recommandations à Desjardins et ont conclu que : « *Desjardins n'a pas fait preuve de la prudence nécessaire à l'égard des données personnelles sensibles qui lui ont été confiées* ».

Sachant que le principal intérêt des institutions bancaires est le profilage, ce n'est pas pour mieux servir le client mais bien pour mieux battre la concurrence qu'ils ont un « si grand appétit » pour nos renseignements personnels.

Mauvaise utilisation de la chaîne de bloc

Le gouvernement s'apprête à utiliser une nouvelle technologie de chaîne de bloc qu'il ne semble pas maîtriser pour stocker les données privées de chaque citoyen, ce qui est hautement inquiétant. (Consultez ce document : <https://www.facebook.com/events/428398245560514>)

D'après nos analyses actuelles, il semblerait que centraliser les données dans une chaîne de bloc ne peut fonctionner sans lui assigner éventuellement une cryptomonnaie. Si le gouvernement persiste dans le choix d'une chaîne de bloc pour stocker les identités numériques, il est donc prévisible qu'ils devront relier le tout à de l'argent. Est-ce pour cette raison que le Mouvement Desjardins s'est enregistré comme lobbyiste dans le portefeuille d'identité numérique ?

L'opacité avec laquelle les choix s'opèrent au Ministère de la cybersécurité et du numérique devrait alerter nos chiens de garde auprès de qui nous avons demandé de faire enquête. Nous sommes en attente d'une décision de leur part.

L'éthique du ministre Éric Caire

Le ministre ne devrait pas être celui qui – tout à la fois – détermine le contenu des lois sur la transformation numérique ET des lois sur la protection des renseignements personnels, qui fait

¹⁰ Les chiens de garde de la vie privée sont très préoccupés pas par le nombre croissant des incidents de sécurité. L'obligation de déclarer ces incidents sont maintenant inscrites dans la majorité des lois de protection des renseignements personnels fédérales et provinciales y compris au Québec, dans le Projet de loi n° 64.

¹¹ <https://www.cai.gouv.qc.ca/communiqu%C3%A9-cai-decision-enquete-desjardins/> et https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2020/nr-c_201214/

des choix technologiques, implante le système, les mesures de sécurité TOUT EN assurant la conformité aux exigences légales de PRP EN PLUS d'en vérifier la légitimité. C'est exactement la position actuelle du ministre. Et le Premier ministre François Legault accepte ce dérapage.

Le ministre de la cybersécurité et du numérique, Éric Caire, a reçu un énorme budget pour mettre en place un projet pour lequel les citoyens n'ont pas été consultés. Québec prévoit 451 millions de dollars pour la transition vers le numérique au cours des cinq prochaines années. Un montant 1,5 milliard de dollars des contribuables est prévu pour favoriser le développement de nouvelles technologies au Québec.¹²

Étrangement, le ministre a été incapable de mettre l'argent des contribuables dans les mains de la Commission d'accès à l'information (CAI), qui est pourtant le chien de garde de leurs données. Il a prétexté que « le peuple trouverait la dépense exagérée... ». La CAI s'est ainsi vu refuser par le ministre Caire - qui rappelons-le est aussi ministre responsable des lois sur la PRP - une somme de 12,4 M\$ supplémentaires à son budget. Ce sous-financement met en péril sa fonction même et sa capacité de bien remplir son rôle¹³. Les priorités du ministre Caire ne peuvent pas être plus claires...

Le ministre s'épargne, de façon pour le moins nonchalante, de faire des évaluations d'impact et des études d'opportunité sur la question de nos données privées, dans un nouvel écosystème bionumérique. La loi et les meilleures pratiques recommandées, normes ou standards reconnus internationalement obligent pourtant à ce principe de prudence selon toutes les pratiques internationales.

Le ministre met en place un nouvel écosystème social qui concerne directement chaque citoyen. Il ne consulte pas réellement la population.

Un sondage de 5 minutes a été fait auprès de la population sur la transformation numérique et 566 personnes y ont répondu. 137 personnes ont contribué au volet *Dialogue - vers le gouvernement du futur*. De plus, une consultation en ligne a été faite auprès du personnel de l'État (5064 répondants.tes)¹⁴

Cela permet-il au ministre d'affirmer haut et fort que les citoyens sont au centre de l'évolution des services, des programmes et des politiques au cœur des projets ?

Le ministre affirme à répétition que les technologies choisies renforcent la sécurité des données personnelles des Québécois.¹⁵

En matière de cybersécurité, a-t-il fait de manière transparente une telle évaluation pour choisir les technologies de la chaîne de bloc, les services infonuagiques et autres qui soient les plus protecteurs des droits des citoyens ? A-t-il cédé aux pressions des entreprises privées telles

¹² Le budget 2022-2023 du gouvernement du Québec prévoit 451 millions de dollars pour la transition de l'État et des entreprises vers le numérique, et pour stimuler les achats de technologies, au cours des cinq prochaines années.

¹³ [Le ministre Caire se fait rabrouer par la Commission de l'accès à l'information.](#)

¹⁴ Sondage de 5 minutes pour contribuer à la transformation numérique gouvernementale

¹⁵ <https://www.quebec.ca/nouvelles/actualites/details/strategie-de-transformation-numerique-gouvernementale-2019-2023-des-services-publics-adaptes-a-la-realite-daujourd'hui-par-une-administration-publique-innovante>

Amazon qui a été la cible de critiques concernant sa collaboration avec les agences de renseignement et de surveillance américaines ?¹⁶

Le ministre ne donne aucune garantie aux citoyens qu'ils demeureront souverains de leurs données personnelles. Au contraire, cette opacité risque d'affecter grandement, à la fois la sécurité de ses données, sa liberté et son autonomie en tant que citoyen consommateur et utilisateur des services de l'État. Le citoyen risque de devenir le grand perdant du portefeuille d'identité numérique québécois.

Le gouvernement affiche une attitude complaisante à l'égard de l'écosystème bionumérique qu'il met en place à toute vitesse. Rien ne justifie une telle précipitation – sauf si le gouvernement a des intentions qu'il n'a pas nommées.

Pas si vite avec le portefeuille d'identité numérique...

Les citoyens n'ont pas voté ni été consultés pour cet écosystème dont la centralisation pose de graves problèmes moraux, d'éthique, de liberté, d'autonomie et de sécurité, ni pour une telle utilisation des fonds publics. La façon de mener ces projets fait fi des bonnes pratiques élémentaires de saine gouvernance et de conformité aux lois sur la PRP.

Rappelons que le premier article de la Charte des droits et libertés de la personne consacre le droit de « *tout être humain a droit à la vie, ainsi qu'à la sûreté, à l'intégrité et à la liberté de sa personne* ».

Le fait de travailler derrière les portes closes contrevient également à l'esprit des technologies qu'il utilise, démontrant que le gouvernement pourrait les utiliser à mauvais escient, volontairement ou non. La Stratégie de transformation numérique gouvernementale 2019-2023 comporte certes, des avantages pour les citoyens par exemple, qu'ils n'aient à communiquer qu'une seule fois leurs informations à l'administration publique, mais tout porte à croire que la voie empruntée par ce gouvernement ouvre la porte à une amplification de la surveillance des citoyens et au crédit social à la chinoise.

Le gouvernement du Québec agit de manière précipitée et sans fondations concernant l'adoption hâtive d'un système d'identification numérique. Le prochain gouvernement devra sérieusement redresser la barre.

Ce que le prochain ministre de la cybersécurité et du numérique devra corriger et promouvoir

Tous les futurs élus seront touchés par le portefeuille d'identité numérique. Ils devront s'assurer que leurs décisions ne violent pas les droits fondamentaux des citoyens.

¹⁶ Amazon fait la pluie et le beau temps dans l'infonuagique. : [...] À Québec, deux personnes sont inscrites au registre des lobbyistes du Québec pour Amazon afin de présenter l'entreprise et ses solutions infonuagiques (cloud) dans le but d'analyser les possibilités que le Conseil du Trésor ou le gouvernement ait recours à ses solutions. [...] Amazon, tout comme ses compétiteurs Google, Apple et Facebook, est également la cible de critiques concernant sa collaboration avec les agences de renseignement et de surveillance américaines.

Le futur ministre de la cybersécurité et du numérique devra faire ses devoirs, notamment vérifier les éléments suivants et en rendre compte publiquement aux citoyens :

- Vérifier que le gouvernement sortant a clairement établi une base de données probantes et les vérifications requises avant de déployer un système d'identification numérique ;
- Vérifier qu'il a fait les études de base, les recherches, les analyses coûts-avantages, bénéfico-risques, des analyses d'optimisation des ressources et des évaluations d'impact en amont des projets, au cours de leur réalisation, lors de leur déploiement, utilisation et évolution.

Actuellement, le ministère de la cybersécurité et du numérique nous semble préoccupé que par la phase de réalisation du projet de portefeuille numérique alors que les dérapages et les risques de PRP et de cybersécurité sont élevés, sinon plus, une fois que ce système d'identité numérique sera mis en service et qu'il ne sera plus mis en lumière comme c'est le cas actuellement ;

- Vérifier qu'il a pris toutes les mesures nécessaires pour prévoir et atténuer les préjudices et qu'il puisse en faire la démonstration de façon objective et impartiale.

La vérification de sécurité et de conformité devrait faire l'objet d'un audit indépendant par une entité externe au projet à toutes les phases du projet y compris après sa mise en service et au cours de son évolution.

Cette centralisation de ses rôles et pouvoirs, ajoutée au fait que le ministre s'est octroyé, par la loi 95, le pouvoir de prescrire quelles données seront recueillies, utilisées et communiquées à des tiers, enfreint les règles élémentaires d'éthique et de saine gouvernance et elle est très inquiétante¹⁷.

Le prochain ministre de la cybersécurité doit décentraliser et rendre les citoyens souverains face à leurs données privées.

Il devra démontrer aux citoyens comment il compte les protéger contre le profilage indispensable au crédit social. En effet, la chaîne de bloc choisie pour stocker les données lui donnera la capacité de traiter à sa guise les renseignements personnels de n'importe quel portefeuille (les modifier, les effacer, les censurer, etc.).

L'enjeu inavoué : la mise en place d'un écosystème bionumérique

Le public n'a pas choisi cette vision du monde bionumérique. Tel est l'enjeu qui devrait se nommer clairement.

Refuser de faire l'étude d'impact de tels écosystèmes ainsi que l'étude des opportunités donne à croire que le tout se passe en vase clos pour servir des intérêts autres que ceux des citoyens. La

¹⁷ Voir à ce sujet le Mémoire de la CAI déposé le 21 mai 2021 lors des travaux parlementaires sur le projet de loi 95 qui indique : « La Commission est convaincue que la transformation numérique de l'administration publique peut et doit s'effectuer dans le respect des principes de protection des renseignements personnels. La Stratégie de transformation numérique gouvernementale 2019-2023 insiste d'ailleurs sur l'importance du consentement du citoyen et sur le respect de la protection de ses renseignements personnels dans l'utilisation de ceux-ci. De l'avis de la Commission, le projet de loi no 95 s'écarte de cet engagement ».

maison du peuple ne peut établir de projet de société sans faire preuve de transparence et sans la participation active et le consentement des citoyens.

Le profilage des citoyens

Sachant que tout l'écosystème bionumérique relève d'abord du ministère de la défense et des renseignements, il est à prévoir que le profilage des citoyens serve à les censurer. Cette dynamique déjà en place ouvre la porte à une forme de totalitarisme.

Les risques sont bien réels et nos inquiétudes sont fondées si on regarde la tendance prise par les gouvernements fédéral et provincial et un peu partout dans le monde ces deux dernières années. Le seuil limite de réduction et de perte de nos droits à la confidentialité de nos données a été plus que franchi : il y a à peine deux ans, il aurait été inacceptable d'être forcé de fournir des données médicales confidentielles les plus sensibles à un employé d'un restaurant qui les consignait dans un registre accessible à tous les employés.

Le gouvernement par simple décret a enfreint les règles élémentaires du consentement libre et éclairé des lois sur la santé qui protègent le secret médical. Il est reconnu que les données médicales et financières sont les plus sensibles. La prochaine étape dans le monde numérique sera-t-elle le partage et l'utilisation de nos données financières sans notre consentement et à notre insu par simple décret faisant fi du caractère prépondérant des lois sur la PRP ? S'agira-t-il de réduire notre autonomie et notre liberté de choix en suivant nos déplacements et notre profil de consommation sous prétexte de la réduction de notre empreinte carbone ? Par exemple, en juillet 2022, au Sri Lanka : une « passe carburant », a été mis en place permettant de bloquer les achats une fois un seuil dépassé¹⁸.

Nos chiens de garde de la vie privée et de la PRP, les élus, cadres de tous les niveaux hiérarchiques ainsi que les organismes de protection des droits des consommateurs doivent comprendre clairement l'écosystème bionumérique dans lequel le gouvernement canadien et le gouvernement québécois actuels semblent être en voie de nous enfermer et doivent protéger les citoyens des dérives potentielles.

Les lois sur la PRP ne peuvent à elles garantir que nos droits sont protégés. Cela nécessite un encadrement rigoureux en amont des projets et des décisions gouvernementales, une transparence et une vigilance constante ainsi que la sensibilisation continue du public aux risques et enjeux.

Si le gouvernement laisse les institutions bancaires bafouer nos lois, anciennes et nouvelles, c'est qu'il fait lui-même fi du respect des droits fondamentaux de citoyens. Ne pas décourager les institutions bancaires et les entreprises devant un abus de demande de données privées fera du gouvernement le complice d'un régime totalitaire. Il se constituera naturellement, malgré nous, si nous n'y prenons garde maintenant.

Vous êtes en campagne électorale ?

En cette année électorale, nous estimons urgent de saisir tous les candidats de la gravité des enjeux, traités avec légèreté et nonchalance par le gouvernement actuel.

¹⁸ Voir à ce sujet : [Le Sri-Lanka instaure un "passe carburant". 26 juillet 2022](#)

Deux visions du monde

Chacun des candidats doit comprendre clairement l'écosystème bionumérique dans lequel le gouvernement canadien et le gouvernement québécois actuel semblent être en voie de nous enfermer.

Les candidats aux élections provinciales doivent conscientiser que le public n'a pas choisi cette vision du monde bionumérique. Or, présentement, il ressort pour qui veut bien voir, pour qui a de l'intuition, pour qui creuse les zones d'ombre, que la société se dirige vers deux visions du monde. L'une humaine et respectueuse des droits et de l'évolution de la personne. L'autre, le profilage bionumérique sous le contrôle de l'état.

En tant que potentiel député, auquel des systèmes aimeriez-vous contribuer pour les citoyens, vous-même ainsi que vos enfants et petits-enfants ?

Des solutions bénéfiques pour les citoyens

Comment redonner à nos chiens de garde les pleins pouvoirs d'agir sur l'écosystème bionumérique afin de protéger les citoyens ?

Voici des pistes de solution :

- L'objectif le plus imminent est que les institutions bancaires, y compris le Mouvement Desjardins, revoient leurs contrats liés aux pratiques et conditions d'accès aux services en ligne et autres. Les clients doivent être en mesure de négocier librement ces contrats. Ils doivent garder la maîtrise des renseignements personnels qui les concernent et être en mesure d'exercer librement une vigilance, cela afin d'assurer notamment que ces institutions ne recueillent et n'utilisent que les données nécessaires en fonction de leurs mandats et des exigences légales. Le contraire les place hors la loi.
- Des moyens concrets doivent être mis en place pour que le citoyen soit partie prenante de ce projet d'environnement bionumérique et de portefeuille d'identité numérique afin qu'il demeure souverain de ses données privées.
- Le portefeuille d'identité numérique doit reposer sur une technologie qui protège la souveraineté du citoyen sur son identité, à savoir qu'il soit le seul à posséder la clé de son identification.
- Le gouvernement ne doit pas confondre les mesures de cybersécurité avec celles reliées au respect de nos droits fondamentaux, à la liberté, à l'autonomie, et de la vie privée ainsi que de la protection de données personnelles. Bien que la cybersécurité soit essentielle, il doit revoir ses orientations et son plan de transformation numérique et sa gouvernance de portefeuille d'identité numérique afin de garantir le respect des droits fondamentaux des citoyens.
- Les organismes de protection du consommateur doivent s'impliquer dans la défense de nos droits dans l'écosystème numérique selon une approche préventive **avant** qu'il y ait atteinte à nos droits. Sinon, nous ne pourrons plus faire marche arrière.

Nous, citoyens, sommes en droit d'exiger que le gouvernement réalisent ses activités en mettant en place les meilleures pratiques internationales recommandées.

Nous exigeons une transparence et un droit de regard public en ce qui concerne les plans, les appels d'offres et la participation du gouvernement fédéral et des autres provinces, des gouvernements étrangers et des organisations internationales, en vue de discussions approfondies dans les forums démocratiques, y compris les médias publics et à l'Assemblée nationale.

La preuve doit être faite que cet écosystème numérique ne portera pas atteinte à l'intégrité et à la liberté individuelle des citoyens ni au respect des autres droits fondamentaux à la vie privée et à la protection des renseignements personnels qui les concernent.

Connexion-U compte sur l'engagement formel des futurs élus d'exercer une vigilance constante pour éviter que nos gouvernements et les entreprises privées soient tentés de tracer leurs citoyens pour toutes sortes de raisons, par toutes sortes de décrets, sous prétexte notamment d'une meilleure cybersécurité et gestion des fonds publics ainsi que d'une meilleure santé publique.

Nous vous invitons à contacter [Connexion-U](#), organisme non partisan dévoué à protéger l'être humain et la démocratie dans l'économie numérique, afin de proposer des solutions satisfaisantes et non discriminantes aux citoyens inquiets du développement de l'identité numérique.

Espérant un dialogue fructueux et à la satisfaction des citoyens dont Connexion-U est le porte-voix, recevez nos salutations respectueuses,

Connexion-U, et tous les citoyens mentionnés dans cet envoi courriel

**Mention : Desjardins a été la première institution bancaire à utiliser une pratique questionnable. Toutes les banques qui utilisent les mêmes inversions de loi pour mettre en place une politique qui force les clients à renoncer à leurs droits fondamentaux sont tout aussi moralement tenues de se justifier.*