CFP - 002M
C.P. - PL 6
Ministère de la
Cybersécurité
et du Numérique

KELVIN ZERO
LA VRAIE NATURE DU NUMÉRIQUE

MÉMOIRE

Sur le projet de loi n° 6, Loi édictant la Loi sur le ministère de la Cybersécurité et du Numérique et modifiant d'autres dispositions

Présenté à la Commission des finances publiques

Kelvin Zéro

Novembre 2021

INTRODUCTION

Kelvin Zéro est une entreprise technologique basée à Montréal composée d'une équipe d'experts ayant une grande expérience dans le domaine des infrastructures critiques, la cybersécurité, la protection de la vie privée, l'échange de données ainsi que l'identification et l'authentification par biométrie. (Voir davantage d'information au sujet de Kelvin Zéro en Annexe)

Nous avons lu avec beaucoup d'intérêt le projet de loi nº 6 dont la Commission des finances publiques est saisie. Nous sommes d'accord avec l'approche générale du ministre responsable, qui vise à centraliser la transformation numérique du gouvernement du Québec au sein d'une seule organisation, le nouveau ministère de la Cybersécurité et du Numérique. Cette étape permettra un développement coordonné des activités du gouvernement dans ce domaine crucial pour l'avenir de ses relations avec les citoyens. Il s'agit d'une opportunité unique pour le Québec de se démarquer à l'échelle nationale et même devenir un leader mondial en construisant une structure efficace, sécuritaire et polyvalente.

Avec l'adoption du projet de loi, une étape significative sera franchie. Cependant, comme le ministre, M. Éric Caire, l'a expliqué, le plus gros du travail reste à faire. Le nouveau ministère aura pour mandat « *d'animer et de coordonner les actions de l'État dans les domaines de la cybersécurité et du numérique.* » Comme partie de ce mandat, le ministère devra notamment « *s'assurer que les organismes publics mettent en place les meilleures pratiques en matière de cybersécurité.* »

C'est cette partie du projet de loi qui nous interpelle. De quoi parle-t-on quand on évoque *« les meilleures pratiques »*? Nous comparerons dans ce mémoire l'approche actuelle de gestion des données à celle que nous avons développée et présenterons nos recommandations. Nous considérons que notre approche s'accorde avec les objectifs du gouvernement dans le projet de loi nº 6 et permettrait une mise en œuvre sécuritaire et efficace de ses dispositions.

1. L'APPROCHE ACTUELLE DE GESTION DES DONNÉES

1.1 Description de l'approche actuelle

Jusqu'à présent, le modèle de gestion d'identité d'un citoyen est toujours le même : les entreprises ou le gouvernement demandent des pièces d'identités et des renseignements personnels dans le but d'identifier un utilisateur ou un citoyen. Une copie de ces renseignements est ensuite enregistrée dans une base de données propre à cet organisme. Cet exercice est répété à chaque fois qu'un individu veut utiliser le service qu'offre cet organisme. Que ce soit pour obtenir une hypothèque, assurer un véhicule, renouveler son permis de conduire, commander un produit ou un service ou encore effectuer une prise de rendez-vous médical, l'individu devra fournir ses renseignements personnels à des organisations qui ne sont pas nécessairement équipées pour protéger ses données ou contrer les autres risques inhérents à l'approche actuelle de gestion des données

1.2 Les risques et inconvénients de l'approche actuelle

L'approche actuelle de gestion des données comporte des risques et inconvénients importants.

D’abord, au fil des années, des dizaines voire des centaines de copies de votre nom, numéro d’assurance sociale (NAS) et autres données confidentielles se retrouvent dans les bases de données d’organisations diverses. Chacune de ces copies devient une opportunité de fuites de données et leur protection est laissée aux soins de ces organisations. À chaque fois que cette information est enregistrée quelque part, les risques que celle-ci soit divulguée par un employé malveillant ou exposée par une cyberattaque sur un système mal protégé augmentent de manière exponentielle.

En plus d’être à risque au repos, ces informations sont à risque chaque fois qu’elles sont transmises d’un système à un autre ou saisies dans une page web. Chaque transfert d’information devient une opportunité pour un pirate informatique d’intercepter ces données et chaque saisie devient une opportunité d’hameçonnage par une page web frauduleuse. Le gouvernement lui-même se soumet aux risques de fuites de données inhérents à cette approche en copiant ses propres informations d’un ministère à l’autre et en redemandant sans cesse les mêmes informations aux citoyens pour utiliser ses services.

Ensuite, cette approche rend la visibilité, la traçabilité et la vérification de l’intégrité de l’information quasi impossible. Par exemple, un acteur frauduleux qui a obtenu suffisamment d’informations volées peut obtenir un nouveau contrat de téléphone cellulaire ou une traite bancaire, à votre nom, sans que personne ne s’en rende compte. Puisque l’information utilisée est véridique, il n’y a aucune mesure en place pour vérifier que c’est bien vous qui effectuez la transaction. Nous avons utilisé de façon publique des informations privées pour s’identifier et s’authentifier, à un point tel que celles-ci ne sont plus si privées et ont perdues leur qualité propre à l’identification et l’authentification. Nous devons à tout prix cesser de fonctionner ainsi.

Finalement, l’approche actuelle engendre des coûts faramineux pour protéger la même information à plusieurs endroits, augmente la complexité de maintenir à jour les bases de données et expose les organisations aux erreurs d’entrées, de frappes et de synchronisation.

1.3 L’approche actuelle dans le contexte du projet de loi nº 6

Deux raisons principales ont été évoquées par le gouvernement du Québec concernant la création du ministère de la Cybersécurité et du Numérique. D'une part, le gouvernement souhaite concentrer les efforts et simplifier l'accès aux services gouvernementaux. Cela passerait entre autres par la mise en place d'une identité numérique, qui permettrait aux Québécois d'éventuellement délaisser leurs documents papier, tels que la carte d’assurance-maladie. D’autre part, le gouvernement souhaite mieux se protéger contre les cyberattaques et les vols de données.

L’atteinte de ces objectifs est largement tributaire du modèle de gestion des données qui sera choisi et mis en œuvre par le gouvernement du Québec. Si la duplication des données subsiste avec l'utilisation de l’identité numérique, cela ne sera qu’une information de plus qui pourra être utilisée contre les Québécois en cas de fuite de données. Si cette identification est liée à une base de données biométriques de citoyens québécois, les dommages seront d’autant plus grands en cas de fuite, en plus de soulever d’énormes questions éthiques et d’acceptation sociale sur le sujet.

2. LA NOUVELLE APPROCHE DE GESTION DES DONNÉES

2.1 Description de la nouvelle approche

Kelvin Zéro propose une approche complètement différente de la gestion des données. Il s'agit de conserver les renseignements personnels des citoyens à un seul endroit, et de faire en sorte que seules des requêtes d'identification et d'authentification du citoyen soient en circulation. L'approche propose également d'utiliser des références à l'information plutôt que de la copier directement.

Nous avons reconnu cette nouvelle façon de faire dans les propos du ministre Caire lors de sa conférence de presse du 28 octobre dernier :

> *« On va donc créer cette identité numérique qui va faire en sorte que chacun des citoyens va devoir, évidemment, démontrer son identité, ensuite va faire partie de l'identification numérique qui va être gérée par le gouvernement du Québec. Donc, vous, M. Laforest, vous allez nous démontrer que vous êtes bel et bien Alain Laforest, on crée votre identité numérique, et, après ça, c'est cette identité numérique là dont vous allez vous servir à travers les différents systèmes. »*

Kelvin Zéro croit fermement que le succès d'un tel système commence par l'établissement de bases solides autour du concept de sécurité de l'information. Avec les avancées technologiques des dernières années en matière de cryptographie, il est maintenant possible d'adopter une approche qui assure l'intégrité de manière mathématiquement vérifiable et qui permette ainsi de diminuer drastiquement le risque de fuites de données. Cela ouvre également la porte à l'utilisation de ces systèmes de façon ouverte, transparente et de manière centralisée ou décentralisée, selon les besoins.

L'approche que nous proposons utilise l'information différemment. Le principe est le suivant : le système demandeur, c'est à dire celui qui cherche à identifier ou authentifier le citoyen, vérifie une hypothèse auprès du système qui émet l'information. Cela évite au demandeur d'avoir l'information en sa possession, tout en lui permettant de vérifier ce qu'il doit vérifier. Avec cette approche, les informations personnelles sont donc utilisées comme point de référence et ne sont plus copiées dans les bases de données de chaque organisation.

Ce nouveau modèle de gestion de l'information permet également de vérifier l'authenticité des transactions en utilisant des clés cryptographiques propres au client. Elles permettent de prouver mathématiquement que c'est bel et bien vous qui autorisez la requête et non quelqu'un d'autre qui possède de l'information volée.

Un exemple simple serait le suivant: avec le système en place, le seul moyen pour la SAQ de vérifier que le client a 18 ans ou plus est de demander une preuve d'identité où se retrouve son nom, sa date de naissance et toutes les autres informations présentes sur la carte. Il est donc possible pour un employé de conserver ses informations pour les utiliser à des fins malicieuses, tandis qu'il est impossible de vérifier la validité de la carte ou celle du détenteur. Avec le nouveau système, la SAQ pourrait simplement demander au client s'il consent à ce que la SAQ vérifie s'il a plus de 18 ans. S'il accepte, le client approuve cette transaction à l'aide de son identité numérique. La SAQ n'a ensuite qu'à vérifier auprès du Gouvernement du Québec si le client a 18 ans ou plus.

2.2 Les avantages de la nouvelle approche

La nouvelle approche que nous proposons a plusieurs avantages concrets, tant pour les citoyens que pour les organisations et le gouvernement. Elle a notamment pour effet de :

- Redonner le contrôle de l'information au citoyen ;
- Libérer les organisations du fardeau de la protection des données ;
- Offrir une méthode sécuritaire et standardisée de gérer l'information à travers la province ;
- Rendre impossible le vol des données lors des communications ;
- Créer une preuve vérifiable que cette transaction a eu lieu, et que c'est bel et bien le détenteur de l'information qui l'a approuvée.

Cela donne place à des économies substantielles à long terme. L'information n'est enregistrée qu'à un seul endroit et ne nécessite donc qu'une seule infrastructure pour la protéger, monitorer et gérer. Cela aura pour effet de diminuer considérablement le volume global de données à sauvegarder et transporter.

C'est vers ce nouveau modèle de gestion des données que se dirigent certaines grandes banques canadiennes par l'entremise de projets pilotes avec Kelvin Zéro. C'est également le modèle adopté par le projet ITEA3 « Secur-e-Health »[1], un consortium de 34 organisations établies dans huit pays, dont Kelvin Zéro est le leader. Le but de ce consortium est de mettre en place un système de ce type pour faire progresser la télémédecine, les études cliniques et le suivi des patients.

Le tout peut également être lié à l'utilisation d'une vérification biométrique. En appliquant le même concept, cette information biométrique devrait être conservée chez le citoyen uniquement. Par exemple, une carte de crédit biométrique ou un téléphone cellulaire peuvent être utilisés pour autoriser une requête d'information de manière cryptographiquement vérifiable, sans que l'information biométrique ne circule. On exploite alors toute la puissance de l'identité biométrique pour identifier le citoyen tout en éliminant le risque de pertes de données.

À l'inverse, si la mise en œuvre de la vérification biométrique se fait en enregistrant cette biométrie de tous les citoyens dans une base de données, ce système deviendra une cible majeure pour les cyberattaques de toutes sortes. Lorsque centralisée, la biométrie devient problématique car elle n'est ni remplaçable ni utilisable en cas de brèche, fuite ou perte. Le tissu de confiance devient brisé de façon permanente. À l'inverse, une référence à usage unique est faite pour être constamment remplacée, peut être non-répudiable et non-corrélable, tout en conservant un lien direct avec une biométrie qui serait idéalement décentralisée.

2.3 La nouvelle approche dans le contexte du projet de loi nº 6

Le gouvernement n'a qu'une seule chance de déployer un tel système et il est impératif que son architecture soit sécuritaire et efficace dès le départ. Une fois un système choisi et mis en place, il sera impossible pour le gouvernement de faire marche arrière. En réunissant des experts dans le domaine et en favorisant les efforts collectifs et les investissements en amont, le gouvernement augmentera

[1] Pour plus de détail sur le projet, visitez https://itea4.org/project/secur-e-health.html

significativement ses chances de faire de ce projet un succès dont tous les Québécois et Québécoises seront fiers.

3. LE SECTEUR PRIVÉ

Nous remarquons dans ce nouveau projet de loi l'absence de mention de collaboration avec le secteur privé ainsi qu'avec les citoyens. Un des concepts fondamentaux de la cybersécurité est que le système est aussi sécuritaire que son maillon le plus faible. Même dans l'éventualité où le gouvernement développe un système parfaitement sécuritaire, celui-ci doit quand même interagir avec d'autres entités et individus à l'extérieur du gouvernement. Dès ce moment, l'intégrité du système est de nouveau compromise

Nous pensons qu'il est important que le ministère de la Cybersécurité et du Numérique travaille de pair avec le secteur privé et les citoyens, afin de rendre l'ensemble du système aussi sécuritaire que possible. Au-delà d'une collaboration au niveau du développement de la solution, il y a une immense opportunité de faire profiter de l'expertise de ce nouveau ministère une fois la solution en place. Étant donné les montants importants qui seront investis à mettre en place cette infrastructure, le gouvernement a tout intérêt à promouvoir les bonnes pratiques en matière de sécurité. En mettant à disposition des outils et des standards, le ministère agirait de manière proactive envers la sécurité de la société québécoise.

CONCLUSION

Avec le projet de loi n^{o} 6 que vous avez devant vous, le gouvernement du Québec va franchir une étape importante : il va se doter d'un centre d'expertise et d'un guichet unique pour la transformation numérique de l'État.

C'est une étape significative, mais ce n'est pas l'étape ultime. Ce nouveau ministère doit maintenant faire les bons choix. Nous avons longuement étudié les différentes façons de protéger les données des citoyens. Nous en sommes venus à la conclusion qu'il faut complètement revoir la façon dont nous tentons tant bien que mal de protéger ces données.

En investissant dès maintenant pour revoir le paradigme de duplication des données, le ministère met toutes les chances de son côté pour que la mise en place du système d'identité numérique et les projets à venir soient faits de manière sécuritaire.

ANNEXE: L'ÉQUIPE KELVIN ZÉRO

Kelvin Zéro est un fournisseur de solutions technologiques qui se consacre à réinventer la façon dont la société interagit avec les données. Nous avons développé un nouveau système et logiciel d'infrastructure permettant aux organisations d'isoler les données sensibles et de distribuer l'accès « Zéro Trust » via une validation cryptographique dites « *sans confiance* ». La mise en œuvre de notre solution complète offre des avantages significatifs en matière de sécurité des données, de gestion de l'identité numérique, de conformité réglementaire, de détection de fraude et de gestion des clés cryptographiques de façon automatisée. Tel que conçu, le système de Kelvin Zéro prend en charge un ensemble complet d'exemples d'utilisation allant de l'identification numérique, de l'authentification et de l'autorisation de cette identité numérique, de la gestion des clés cryptographiques et des portefeuilles numériques ainsi que la transformation numérique complète.

Kelvin Zéro est fière d'être à 100% Canadiens, avec la majorité de son équipe basée au Québec. Notre équipe est formée par des experts en cybersécurité et sont représentatifs de la diversité de notre pays. Leur expérience impressionnante inclut la défense de notre pays et de ses infrastructures critiques.

Thierry Gagnon

Co-fondateur, chef de l'exploitation et chef de l'information de Kelvin Zéro et un expert mondial en matière de réseaux de partage d'information sécurisés. En tant que chef de l'information, il a assemblé une équipe inégalée d'experts soigneusement choisis afin d'aider Kelvin Zéro à franchir la prochaine étape pour les systèmes de données. Avant d'œuvrer chez Kelvin Zéro, Thierry a développé une expertise en bases de connaissances cybernétiques, l'analyse de maliciels ainsi que le renseignement sur les cybermenaces. Au cours de cette période, il a été engagé auprès d'organisations d'infrastructures critiques, autant dans le secteur privé que public, incluant les forces de l'ordre, une agence de cryptographie et de défense nationale, et de la réponse cybernétique nationale.

Arman Afkhami

Vice-Président ventes et marketing chez Kelvin Zéro depuis près de 3 mois, Arman a œuvré majoritairement dans le domaine de l'événementiel et dans le monde de l'art et la culture. Il a notamment travaillé près de 12 ans pour le groupe Juste pour rire en tant que directeur national des partenariats. Son expertise en ventes et marketing amène une dimension nécessaire au groupe afin de sécuriser la croissance de l'entreprise et de lui donner une voix et une image à la hauteur de ses effectifs et de ses avancements technologiques. Dans ces temps libres, il est mentor dans le domaine des arts et de la culture avec l'association Business in Arts et il est également animateur d'évènements.

Louis-David Coulombe

Directeur des Partenaires Techniques, Louis-David possède une expertise de développement et de mise en marché de système d'informatique dans plusieurs secteurs hautement réglementés. En tant qu'ingénieur, il a participé à l'élaboration de projets aérospatial en collaboration avec l'Agence spatiale Européenne (ESA). Plus récemment, il était à la tête de l'équipe multidisciplinaire en charge du développement d'un dispositif médical déposé à la Food and Drug Administration (FDA). Son mandat chez Kelvin Zéro est d'accompagner les différents partenaires et clients dans l'adoption de ses nouvelles technologies de sécurité de l'information.