

Perspectives du CTIC sur une stratégie pour l'économie de données

Sommaire

Le présent livre blanc expose les perspectives du CTIC sur une stratégie pour l'économie de données à une époque où une économie guidée par les données est un facteur de motivation mondial pour les nouveaux entrepreneurs et les industries émergentes qui désirent créer et commercialiser du nouveau contenu de propriété intellectuelle afin de réaliser leurs aspirations nationales, économiques et sociales.

Innovation : La capacité du Canada de participer pleinement à une course mondiale guidée par les données dépendra grandement de notre capacité comme nation d'offrir de nouvelles innovations en matière de données ouvertes tout en protégeant la vie privée du public, en améliorant la sécurité et en favorisant une croissance inclusive.

Il faudra créer un délicat équilibre entre les intérêts économiques, démocratiques et privés qui régiront la libre circulation de l'information au-delà des frontières tout en maintenant l'avantage intellectuel concurrentiel du Canada dans une économie mondiale.

Le paysage d'innovation des données ouvertes du Canada doit être étayé par une stratégie technologique qui se fonde sur des normes favorisées par une interface de programmation ouverte qui permettent aux joueurs tiers de bâtir l'écosystème d'applications et de services pour les Canadiens en dehors des limites d'un environnement propre à un fournisseur notamment dans les secteurs de la santé, du commerce, des services bancaires, du transport.

Protection de la vie privée et confiance : Les incidents touchant la protection des données et les problèmes relatifs à la protection des renseignements personnels qui ont été hautement médiatisés ont affaibli la confiance du public dans la capacité des secteurs public et privé de recueillir, de gérer et d'analyser de façon responsable des renseignements personnels. L'environnement créé par le *Règlement général sur la protection des données* (RGPD) de l'Union européenne a motivé le Canada à examiner sa propre législation en matière de données et de protection de la vie privée et le CTIC recommande des mesures pour mieux gérer les mécanismes de consentement, de notification d'incidents touchant la protection des données et d'application de la loi, ainsi que l'importance des droits relatifs à la portabilité des données.

L'avenir du travail : Les prévisions du marché du travail du CTIC indiquent une demande pour doter 216 000 postes essentiels en TIC d'ici 2021, et la croissance de l'emploi dans le secteur des TIC dépasse celle de l'économie globale dans une proportion de six pour un. Parallèlement, les emplois non liés au domaine du numérique sont remplacés par l'intelligence artificielle, des robots et d'autres technologies perturbatrices. Des initiatives nationales exhaustives de développement des compétences sont nécessaires pour maintenir et améliorer la capacité concurrentielle du Canada en matière de données et de numérique.



Le CTIC affirme que l'élaboration d'une « stratégie nationale sur les données » soigneusement conçue pour le Canada est un important incitatif pour exprimer les aspirations du Canada dans ce domaine et ouvrir la voie à l'investissement, à la croissance et la prospérité sociale.

Introduction

Alors que l'utilisation et la pertinence de la technologie dans l'ensemble des secteurs de l'économie augmentent, le secteur économique numérique s'est transformé en une économie florissante presque indépendante. Il y a quelques années seulement, une manchette appelait les données « le nouveau pétrole », l'identifiant effectivement comme une ressource naturelle virtuelle renouvelable indéfiniment. Pourtant, en raison de développements clés dans le domaine numérique, comme l'infonuagique, l'intelligence artificielle, la technologie de cinquième génération, la réalité augmentée, l'Internet des objets et la chaîne de blocs, le concept même des données a subi une transformation. Les données sont maintenant façonnées en produits finis (courtiers en données combinant des sources de données multiples en de nouveaux produits), monnaies (cryptomonnaies) et composantes de la gouvernance civique (villes intelligentes).

L'accroissement de l'utilisation des données ne devrait pas être le seul but puisque pour atteindre son plein potentiel, l'économie numérique a besoin d'un solide écosystème d'interfaces de programmation ouverte pour rationaliser et institutionnaliser une collaboration numérique entre tous les secteurs de l'économie. Le Canada doit également envisager de quelle façon il protégera la propriété intellectuelle canadienne dans l'économie numérique ainsi que les droits des citoyens en matière de données, un peu comme le fait l'application par l'Union européenne du bouclier de protection des données Union européenne-États-Unis. Alors que l'économie numérique se développe, les organismes canadiens de réglementation de la concurrence et les législateurs doivent s'assurer qu'une économie saine, concurrentielle et novatrice s'établit. La protection de la neutralité d'Internet est l'un de ces enjeux stratégiques et réglementaires qui doivent être renforcés puisque la croissance inclusive sera la marque d'une économie numérique canadienne florissante.

Alors que l'économie numérique prend de l'ampleur et de la vitesse, de nouveaux défis et considérations feront leur apparition pour les gouvernements et les organismes de réglementation. Les manchettes comme celles traitant de l'utilisation des données par Facebook et ses liens avec Cambridge Analytica, la hausse et le raffinement des cyberattaques, et le malaise du grand public à l'égard des données massives contribuent tous à faire de la gouvernance et de la réglementation des données une priorité absolue, mais également une priorité stratégique centrale. Le RGPD de l'Union européenne (Union européenne, 2018) est une mesure hâtive exhaustive, quoique imparfaite, en matière de protection des données. Bien que la protection des droits des utilisateurs et de leurs données soit l'un des fondements de la réglementation, certains aspects du *Règlement* sont assez punitifs pour les entités commerciales. Aussi, ils n'ont pas seulement un impact sur les pays membres de l'Union européenne, mais aussi sur tous les pays qui font des affaires avec ces pays membres. Le Canada est particulièrement touché puisque le récent accord commercial entre le Canada et l'Union européenne, l'Accord économique et commercial global, exigera que bon nombre d'entreprises canadiennes respectent le RGPD. La compréhension de ces exigences est un premier pas. L'élaboration de politiques qui trouvent le juste milieu entre la réglementation relative aux données et la promotion de l'innovation numérique est impérative.

Les stratégies de talents du Canada (fiscales, financières et culturelles) et les politiques sur la concurrence devront également répondre à cette nouvelle réalité qui est de plus en plus considérée comme étant « le nouveau pétrole ».

L'innovation à l'ère des données

De nombreux facteurs doivent être pris en compte lorsque vient le temps de discuter de l'innovation canadienne dans l'économie numérique. Cependant, il importe d'abord de se concentrer sur les segments de l'économie numérique dans lesquels le Canada peut être concurrentiel de manière viable. La répartition trop large des ressources peut mener à l'élaboration de politiques qui sont difficiles à mettre en œuvre ou qui sont inefficaces.

Intelligence artificielle

Le Canada dispose d'une importante fenêtre de possibilité en matière d'intelligence artificielle grâce à son leadership actuel dans la communauté de recherche et le milieu universitaire. Toutefois, en raison des investissements que les concurrents comme la Chine et les États-Unis (Boyd, 2018) réalisent dans le domaine de l'intelligence artificielle et la recherche, cette fenêtre risque de rapetisser au fil du temps. Nous pouvons en profiter maintenant en choisissant des secteurs, des produits et des services d'intelligence artificielle qui nous aident à produire des produits encore meilleurs et plus concurrentiels que ceux de nos concurrents internationaux. Le Canada jouit d'une réputation internationale d'expertise dans des secteurs comme la gestion des ressources, l'agriculture, la sécurité de l'approvisionnement alimentaire et les services gouvernementaux.

Système bancaire ouvert

Alors que l'intelligence artificielle est un point fort pour le Canada, le pays traîne lamentablement derrière ses concurrents internationaux dans certains autres segments importants de l'économie numérique. Le système bancaire ouvert en est un. Les pays qui ont adopté le système bancaire ouvert (permettant aux clients d'ouvrir leurs données bancaires à des fournisseurs de services tiers) (PWC UK, Open Data Institute, 2018) ont vu surgir une industrie offrant ces services tiers et concevant les technologies pour les supporter. Bien que le Canada n'appuie présentement pas directement le système bancaire ouvert, le budget de 2018 (Shecter, 2018) incluait une recommandation pour revoir cette position.

Le mouvement du système bancaire ouvert est un exemple de la portabilité des données en tant que moteur d'innovation, et pas seulement comme un impératif de la protection de la vie privée. Les industries comme les finances, les télécommunications, les soins de santé et les transports pourraient voir une hausse des niveaux de service, ouvrant la porte au développement de nouveaux secteurs complémentaires si la portabilité des données est adoptée en tant que catalyseur de l'innovation.

Interface de programmation ouverte

En général, le Canada n'est pas un pionnier de l'adoption précoce des technologies de transformation. Le système bancaire ouvert est l'un des nombreux secteurs du mouvement ciblant l'interface de programmation ouverte. Il vise à sensibiliser davantage et à accroître l'adoption des interfaces programmatiques entre les applications au sein des organisations et, surtout, entre elles. Les interfaces de programmation ouverte font de la portabilité des données un service durable et inestimable pour les citoyens et les consommateurs. Le mouvement, en plus d'une initiative de normes complémentaires,

peut accélérer l'innovation dans l'économie numérique et aider à différencier les organisations et les pays participants des sociétés et des économies plus fermées.

Propriété intellectuelle de l'économie numérique

Alors que le Canada développe son économie numérique, des mesures de protection doivent être mises en place relativement à la propriété intellectuelle développée par les entreprises canadiennes. L'Europe explore présentement un « droit de propriété des données *sui generis* » pour gérer la propriété intellectuelle en matière de données. Les mesures de protection peuvent s'harmoniser avec les droits individuels de propriété des données et la portabilité des données. Une approche universelle de la protection de la vie privée et de la propriété intellectuelle dans l'économie numérique n'est pas viable et n'est pas non plus la solution idéale pour le Canada. Le Canada peut assumer un rôle de leadership en matière de propriété intellectuelle en créant un carrefour d'échange en la matière pour faciliter l'accès à de multiples actifs canadiens de propriété intellectuelle par le biais de contrats normalisés d'utilisation et de licence.

Politique sur la concurrence

Une autre dimension à considérer est le rôle de la politique sur la concurrence et du Bureau de la concurrence Canada dans le succès de l'économie numérique canadienne. Les monopoles en matière de données et la distribution déséquilibrée du pouvoir de marché ne peuvent qu'empêcher la participation des consommateurs et des entreprises du Canada à l'économie numérique. Le Canada doit élaborer une politique nationale sur la concurrence géographique et sectorielle pour guider le développement d'une économie numérique ouverte et novatrice.

Le Canada doit également examiner l'économie numérique en adoptant un regard de neutralité du Net et continuer d'encourager la création d'un environnement d'échange de données ouvert et sans palier pour favoriser l'inclusivité, l'innovation et la croissance durable des entreprises canadiennes.

Favoriser les investissements privés dans l'économie numérique

Si les données sont réellement le « nouveau pétrole », il est important de tenir compte des mécanismes d'incitation utilisés dans les secteurs des ressources traditionnelles afin de promouvoir les investissements du secteur privé dans l'économie numérique. Les instruments comme les actions accréditatives et les autres incitatifs fiscaux pourraient étendre l'économie numérique au-delà de quelques joueurs bien établis et accroître la viabilité des entrepreneurs sur le marché.

Protection de la vie privée et confiance

La protection des données et des informations communautaires individuelles et vulnérables est un défi en perpétuelle évolution. Les avancées touchant les dispositifs personnels, y compris la portée tentaculaire des médias sociaux dans la vie de tous les jours et le déploiement rapide des services numériques dans les secteurs public et privé, ne font qu'amplifier la nécessité que les établissements publics et privés disposent de mesures de protection de la vie privée et de pratiques exemplaires rigoureuses et évolutives.

Il est important pour le Canada de combler les écarts entre le RGPD de l'Union européenne et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) (Gouvernement du Canada, 2018), en plus des contreparties provinciales. Les facteurs clés dont il faut tenir compte dans le cadre de ce processus sont les suivants.

Consentement : La LPRPDE énonce des règles relativement strictes en matière de consentement, alors que le RGPD est plus flexible. La LPRPDE précise que le consentement est le *seul* fondement permettant de recueillir et de traiter des renseignements personnels, alors que l'article 6.1 du RGPD énonce six cas dans lesquels des données peuvent être légitimement traitées, dont seulement un en vertu d'un consentement.

Cependant, de nombreuses discussions et recherches portent sur la pertinence des modèles fondés sur le consentement. La philosophe de la protection des renseignements personnels numériques Helen Nissenbaum (Berinato, 2018) s'est prononcée contre les principes de base du modèle de consentement numérique, citant comme motifs clés la fausse impression d'exercer un contrôle réel et le consentement comme n'étant simplement pas des mesures de la protection de la vie privée. Inversement, d'autres intervenants comme la professionnelle des données responsables Alix Dunn (Anna Scott, 2018) proposent une éthique agile comme modèle à intégrer dans les modèles de protection de la vie privée. Alix Dunn définit l'éthique agile comme suit : « Le but de l'éthique agile est de faciliter le travail éthique accéléré. Il s'agit d'une pratique qui peut fonctionner en tandem avec le développement agile. » (Dunn, 2018)

Les récentes manchettes concernant Statistique Canada demandant des données personnelles bancaires auprès d'institutions financières ont attiré l'attention sur la *Loi sur la statistique*. Teresa Scassa, professeure à l'Université d'Ottawa qui se spécialise dans le droit de l'information, a souligné les problèmes découlant de l'utilisation de la *Loi sur la statistique* à l'ère numérique.

« La *Loi* a été rédigée dans une ère analogue. Elle parle de la nécessité pour les organisations de fournir des documents et des dossiers. Elle inclut maintenant des documents et des dossiers numériques.

« Le monde analogue avait des limites inhérentes quant à ce qui pouvait être réalisé. Il y a des limites à la quantité de documents qu'il est possible de transférer. Les incidents touchant la protection des données sont une préoccupation importante et réaliste. » (Russell, 2018) [traduction]

Ce contexte nécessite l'élaboration de cadres clairs qui énoncent des réponses appropriées. Les Canadiens ont besoin d'un cadre législatif national de consentement à l'utilisation des données non seulement pour protéger leurs droits, mais aussi pour préciser les différences entre la LPRPDE et la réglementation provinciale en matière de protection de la vie privée, dont certaines peuvent être difficiles à compartimenter. Le cadre de consentement devrait également renfermer divers niveaux sur les risques relatifs et potentiels associés à des catégories précises de données personnelles (consommation, santé, lieu géographique, religion, politique, etc.), ainsi qu'au besoin d'établir l'impératif des données pour offrir un service ou un produit précis au particulier et de déterminer si la demande de consentement peut réellement être considérée comme éclairée selon les normes ou les références appropriées.

Incidents touchant la protection des données : La LPRPDE et la *Loi sur la protection des renseignements personnels numériques* (Gouvernement du Canada, 2018) offrent un cadre qui exige que les incidents touchant la protection des données soient signalés au commissaire à la protection de la vie privée du Canada, en plus des personnes touchées, lorsque l'incident représente un risque réel de préjudice. Par contraste, le RGPD contient des protocoles stricts en cas d'incident et des amendes administratives connexes en cas de non-conformité (lesquelles peuvent être élevées), mais il n'exige pas le même niveau de notification individuelle que la LPRPDE. En faisant de la LPRPDE une loi évolutive et agile qui peut être rapidement mise à jour afin d'évoluer au fil de la technologie, des cybermenaces et de la confidentialité exigée par la population canadienne en matière de protection de la vie privée, le Canada serait mieux préparé à traiter des défis de cybersécurité et à intervenir.

De plus, les efforts concertés entre les organismes d'application de la loi, les organismes de renseignement, les organismes de cybersécurité et les organisations de gestion numérique des données sont essentiels. Alors que les cybermenaces et les cyberattaques sont de plus en plus répandues et fréquentes, il ne s'agit pas de savoir *si* une organisation sera la cible d'une telle atteinte, mais plutôt *à quel moment*. Cette coordination collaborative peut commencer par des protocoles de sensibilisation, d'éducation et d'intervention en cas d'incidents. Par exemple, ce n'est pas nécessairement toujours souhaitable d'interrompre un incident avant de faire appel aux organismes d'application de la loi et à d'autres intervenants. En réalité, souvent, ces organismes pourraient avoir besoin de laisser un incident suivre son cours pour déterminer si les agresseurs et la réelle intention de l'attaque (comme les attaques pour rançon qui agissent comme des diversions à des attaques plus étendues) peuvent être identifiés.

Le Canada devrait établir un mécanisme contraignant en ce qui concerne les incidents touchant la protection des données. À défaut de le faire, des effets néfastes pourraient se faire sentir : les entreprises pourraient notamment minimiser la portée ou l'impact de tels incidents. Le Canada doit disposer d'un organisme de réglementation responsable de la gestion des plaintes et de la vérification localisée des différents incidents signalés périodiquement, et imposer des amendes aux entreprises lorsque nécessaire. Les modèles à envisager incluent la North American Electric Reliability Corporation (NERC, sans date) et le [mécanisme de plaintes du CRTC](#).

Portabilité des données : Le RGPD exige une portabilité des données pour les particuliers, potentiellement l'exigence la plus percutante pour les entreprises canadiennes. L'article 20 (Union européenne, 2018) exige que les entreprises fournissent aux particuliers les données qu'elles détiennent à leur sujet dans un format structuré et lisible par une machine, leur permettant de les gérer elles-mêmes ou de les transférer vers un autre fournisseur de services. La LPRPDE n'exige pas la portabilité des données. Bien que certaines entreprises canadiennes aient initialement de la difficulté à accepter cette exigence, au bout du compte, les Canadiens devraient avoir le droit de fermer leur compte auprès d'une entreprise et de transférer leurs données ailleurs. L'intensification de la concurrence parmi les fournisseurs de services est un important sous-produit d'une telle politique. Essentiellement, la portabilité des données peut encourager les entreprises à rivaliser pour séduire les clients et gérer leurs données afin de ne pas perdre accès à d'incalculables renseignements dans un environnement où les données sont une monnaie d'échange. En utilisant les dispositions du RGPD comme point de départ, le Canada devrait créer un mécanisme de réglementation pour exiger la portabilité des données.

Le droit à l'oubli : Les Canadiens devraient pouvoir supprimer légalement leurs renseignements personnels s'ils jugent qu'ils ont été modifiés, utilisés à mauvais escient ou affectés négativement d'une quelconque façon. La capacité de supprimer les renseignements personnels d'un contrôleur des données (Google, Facebook, etc.) s'avère toutefois complexe. Ce processus se heurte au premier amendement de la Constitution des États-Unis (Abrams, 2018), et les politiciens, les entrepreneurs et les criminels pourraient s'en servir pour camoufler des activités et des actions antérieures que le public devrait avoir le droit de connaître. Le RGPD (Union européenne, 2018) précise les modalités d'application du droit à l'oubli alors que la législation canadienne actuelle ne contient aucune disposition à cet égard. Une chose est claire : une approche universelle en matière du droit à l'oubli n'est ni plausible ni appropriée. Par exemple, une approche générale serait inappropriée pour les cas touchant les personnes mineures. Ici, un cadre réglementaire qui permettrait le droit à l'oubli pour les jeunes de moins de 18 ans devrait être envisagé, alors qu'il ne serait pas toujours raisonnable de le faire pour les personnes majeures. Une enquête préliminaire du Sénat relativement à la pertinence du droit à l'oubli selon le contexte canadien serait toutefois un premier pas fort bienvenu.

Renseignements personnels des employés : Le RGPD (Union européenne, 2018) contient des exigences générales en matière de collecte et de traitement des renseignements personnels des employés. À l'inverse, la LPRPDE s'applique seulement à un petit groupe d'employeurs sous réglementation fédérale. Tous les autres employeurs sont sous réglementation provinciale, et seulement un certain nombre de provinces mettent en application les considérations en matière de protection des renseignements personnels des employés. Les problèmes découlant de cette incohérence réglementaire peuvent être exacerbés par l'émergence de l'économie des petits boulots, un phénomène qui dépasse les frontières nationales et provinciales et qui fait en sorte qu'il est de plus en plus difficile d'établir une définition claire des personnes qui doivent être considérées comme des « employés ». Le Canada doit agir rapidement afin d'harmoniser les lois fédérales et provinciales en matière de protection des renseignements personnels des employés et de sensibiliser le secteur privé aux conséquences de la conformité du RGPD à la réglementation sur la protection des renseignements personnels des employés.

Le secteur économique numérique, avec ses bons et ses mauvais côtés, ne respecte pas les frontières traditionnelles. Et au bout du compte, la propagation et l'adoption de la technologie numérique dépendent de la confiance et de l'acceptation de l'utilisateur.

Le Canada peut adopter un rôle de leadership en matière de protection des données et de confiance en soutenant l'élaboration d'un cadre international collaboratif et adaptable de protection de la vie privée, qui préciserait les normes en matière d'utilisation des renseignements personnels et des données commerciales. Toute initiative en faveur de ce programme doit également être intégrée au Centre canadien pour la cybersécurité. Le choix des pratiques exemplaires et des normes en matière de technologie et de données doit découler d'une initiative intergouvernementale, soutenue par nos partenaires internationaux.

Une première étape pourrait comprendre une collaboration entre le Canada, le Royaume-Uni, la Nouvelle-Zélande et d'autres [partenaires du réseau numérique D7](#) pour le respect du RGPD et l'amélioration de la LPRPDE et ses contreparties provinciales. Tous ces travaux favoriseraient la protection des droits en matière de données de la population canadienne tout en soutenant une

approche de marché de la réglementation du numérique. Du coup, la collaboration du Canada en matière de cybersécurité au sein du Groupe des cinq (FVEY) pourrait mener à des mesures de protection plus strictes et plus solides de son infrastructure de protection de la vie privée, ce qui, en retour, pourrait renforcer et rétablir la confiance de la population canadienne envers la capacité de protection de la vie privée du gouvernement.

Le nouvel Accord États-Unis-Mexique-Canada (AEUMC) (États-Unis, Mexique, Canada) offre un chapitre sur le commerce numérique et propose aux parties d'examiner les principes et les lignes directrices de la Coopération économique Asie-Pacifique (APEC) et l'OCDE. Les États-Unis doivent également composer avec le bouclier de protection des données UE-États-Unis, et comme l'Union européenne vérifiera, au cours des quatre prochaines années, la LPRPDE à des fins d'adéquation dans le cadre du RGPD, le Canada doit agir proactivement afin de protéger les participants à l'économie numérique canadienne contre les effets négatifs sur la réglementation, le traité ou la conformité.

L'importance de la confiance ne peut pas être sous-estimée. Le Baromètre de confiance Edelman 2018 (Edelman, 2018) indique une détérioration de la confiance envers les gouvernements, les entreprises et les médias. Même si le sondage et la diffusion de ses résultats ont eu lieu préalablement aux derniers développements tels que la fuite de données Facebook-Cambridge Analytica, il met en évidence les préoccupations sous-jacentes de nombreux Canadiens relativement à l'utilisation de leurs renseignements personnels par différents établissements. Le gouvernement du Canada doit collaborer avec le secteur privé et la société civile afin de contribuer à l'établissement d'un écosystème de l'information digne de confiance, que tous adopteront et qui permettra à la population canadienne de l'exploiter à des fins d'innovation et de bien collectif.

Les données ouvertes sont une composante fondamentale du cadre de rétablissement de la confiance. Les données ouvertes peuvent permettre aux organisations de la société civile (ONG, œuvres de bienfaisance et OSBL) de mieux desservir la population canadienne et de fournir aux entreprises des occasions d'innover et de développer de nouveaux produits et services. Les données sur la passation de marchés ouverts peuvent, en particulier, offrir des possibilités de marchés publics aux petites et moyennes entreprises nationales, leur permettant ainsi d'améliorer leur résilience en situation de concurrence et d'aider à financer leur innovation et leur croissance.

L'avenir du travail

D'ici 2021, le Canada sera confronté à une importante pénurie de 216 000 travailleurs dans l'industrie du numérique (McConnell, 2018). Parallèlement, plusieurs partagent de véritables préoccupations quant à la suppression d'emplois non liés au domaine du numérique au sein de l'économie numérique. Lorsqu'il est question d'une approche globale face à la suppression d'emplois, le Canada est quelque peu défavorisé par rapport à ses pairs puisque l'éducation est une compétence essentiellement provinciale. L'éventuelle asymétrie à l'échelle des provinces peut poser problème lorsque vient le temps de développer une réponse globale à la pénurie nationale de compétences.

Le Canada, comme bien d'autres pays, a également de la difficulté à attirer les jeunes dans les domaines des STIM (sciences, technologie, ingénierie et mathématique). Ce problème est souvent amplifié chez

les femmes et les peuples autochtones, qui continuent d’être sous-représentés dans les domaines des STIM et du numérique. L’inclusion, la diversité et l’accessibilité doivent être au cœur de notre programme numérique.

Possibilité

Le Canada peut toutefois faire preuve de leadership en établissant un écosystème de microaccréditation robuste et fiable. Alors que des chefs de file comme IBM, Google et Apple commencent à s’écarter de la nécessité d’embaucher des employés détenant des diplômes d’études postsecondaires (Connley, 2018), le monde tente également de délaisser les méthodes d’accréditation et les désignations professionnelles traditionnelles. Les cours en ligne à la demande comblent souvent l’écart pour les travailleurs existants et futurs du domaine du numérique qui doivent se recycler ou se perfectionner afin de répondre aux exigences de l’industrie. Pourtant, peu de mécanismes sont en place pour vérifier et approuver le contenu des cours ou la véracité du niveau de compétence des participants. L’obtention de ces attestations subdivisées se nomme la microaccréditation. Le Canada peut faire progresser le système en collaborant avec le secteur privé, les OSBL et les organisations de gestion des accréditations telles que Comptables professionnels agréés du Canada et Ingénieurs Canada afin d’établir une plateforme de microaccréditation viable et fiable.

Les avantages à en retirer sont immenses. La microaccréditation peut aider les travailleurs existants à demeurer compétents et permettre la transition de travailleurs d’autres domaines vers le numérique. Et les avantages ne s’arrêtent pas là. La microaccréditation peut également faciliter l’accès au domaine du numérique des peuples autochtones des régions urbaines et éloignées, en les aidant à acquérir les compétences numériques recherchées. Elle peut également profiter aux personnes handicapées, qui pourraient vouloir participer à l’économie numérique, mais qui ne connaissent pas le cheminement adéquat pour y parvenir. Alors que le gouvernement et l’industrie expérimentent l’embauche à la demande par l’intermédiaire d’initiatives comme le Nuage de talents du GC (École de la fonction publique du Canada, 2018), la capacité de vérifier les compétences et les accréditations des candidats deviendra de plus en plus pressante et pertinente. L’adoption d’un cadre préliminaire pour le faire accordera aux entreprises canadiennes un net avantage au sein de l’économie numérique internationale.

Défi

L’un des principaux défis que devra affronter le gouvernement du Canada est la disponibilité de données granulaires et fiables, essentielles à l’établissement d’un système précis de renseignements sur le marché du travail pour l’économie numérique. Actuelle, Statistique Canada fournit des résultats des enquêtes mensuelles sur la population active (Statistique Canada, 2018) selon les codes suivants :

- les codes de la Classification nationale des professions (CNP);
- le système de classification des industries de l’Amérique du Nord (SCIAN).

Même si elles servent à dresser le portrait général des tendances historiques de l’industrie et de la main-d’œuvre sur le plan macroéconomique, ces méthodes de classification peuvent parfois s’avérer désuètes et d’un niveau trop élevé pour une promotion et une planification économiques numériques précises et prospectives. Il existe un besoin criant pour un cadre de codage plus souple et adaptable qui permettrait l’analyse de tendances précises des sous-industries à croissance élevée telles que la fabrication avancée

et les systèmes autonomes, ou des sous-professions recherchées comme les analystes de données et les spécialistes de la cybersécurité. Ainsi, le gouvernement du Canada pourrait mieux planifier les initiatives économiques et faire la juste promotion du Canada en tant que destination de choix pour des investissements internationaux précis dans le secteur numérique. L'Union européenne met présentement à l'essai un cadre de Classification européenne des aptitudes/compétences, certifications et professions (ESCO) (ESCO, 2018). L'une des composantes de base de ce projet pilote est la souplesse du système de classification.

« Afin d'obtenir un niveau de détail plus précis dans le cadre de l'ESCO, par exemple pour des secteurs économiques précis, les piliers liés aux professions et aux compétences peuvent être élargis. Voilà qui s'avère utile pour le développement d'applications très précises propres à un secteur, notamment le jumelage d'emplois et de travailleurs, la planification de la main-d'œuvre et les outils d'orientation professionnelle pour un secteur économique précis. » (Commission européenne, 2018) [traduction]

La souplesse du secteur économique numérique, selon un cadre adéquat, aurait une valeur inestimable pour les entreprises et les gouvernements canadiens.

Autres occasions d'innovation et de protection des renseignements personnels

La LRPDE et la *Loi sur la protection des renseignements personnels numériques* offrent certainement bon nombre d'avantages, mais également quelques désavantages, comparativement au RGPD. Au sens du RGPD, il incombe essentiellement aux particuliers de gérer la confidentialité des données, et par conséquent, la conformité lui incombe aussi, une tâche qui peut s'avérer difficile pour plusieurs. Les représentants de données deviennent alors particulièrement pertinents puisqu'ils peuvent réduire le fardeau lié à la gestion des données. Ce rôle combine l'assistant numérique personnel et le conseiller juridique, mais il est adapté aux particuliers. Ces derniers n'auront ainsi pas à se préoccuper de la réglementation et de l'accès non autorisé aux données autant que nous devons le faire. Une économie analogique non numérique serait le rôle des avocats-fiscalistes, mais ce service serait numérique, gratuit et offert en arrière-scène. Cela étant dit, ce rôle devra être développé et normalisé avec l'aide et la surveillance des autorités de certification, des associations professionnelles et du gouvernement. Voilà une belle occasion pour le Canada de prendre l'initiative, ce qui pourrait donner lieu à des possibilités de croissance et d'exportation de produits et de services qui appuient cette nouvelle économie numérique.

Les fiducies de données constituent une autre bonne occasion. Le Canada peut éviter certains obstacles liés à l'économie numérique en établissant un cadre de gouvernance pour les fiducies de données plutôt que d'attendre qu'un ensemble de règlements disparates concernant les fiducies de données se développe organiquement. Les fiducies de données sont un mécanisme servant à établir des règles de base pour accéder à des collectes de données et les traiter. Par exemple, un projet de ville intelligente pourrait créer une fiducie de données pour protéger le droit du public et de la ville d'accéder aux données recueillies par la plateforme de collecte de données de la ville intelligente. Les fiducies de données peuvent également être structurées de façon à stimuler l'innovation en établissant des règles de gouvernance pour les ensembles de données accessibles aux entreprises en démarrage ou bien

établies. Grâce à l'essor des villes intelligentes et de leurs fonctionnalités comme les grilles en réseaux, les fiduciaires de données devraient être intégrés à tous les processus d'approvisionnement connexes.

Résumé des recommandations stratégiques

Innovation

1. Adopter une réglementation en matière de portabilité des données, non seulement pour traiter des enjeux liés à la protection des renseignements personnels, mais également pour stimuler l'innovation. Le système bancaire ouvert est manifestement la première étape, mais toutes les industries pourront profiter de la portabilité des données et accroître leur résilience en situation de concurrence, et ce, autant à l'échelle internationale que nationale. Ce processus nécessitera une intervention législative afin d'inclure les droits en matière de portabilité des données, le soutien réglementaire et l'application de la loi.
2. Instaurer des programmes fédéraux pour créer et déployer des initiatives d'interface de programmation ouverte afin d'établir une économie numérique saine et en pleine croissance.
3. Élaborer des politiques et une infrastructure en matière de protection de la propriété intellectuelle qui appuient les principes de l'économie numérique.
4. Créer un cadre stratégique fédéral en matière de concurrence qui favorise la réussite des entreprises numériques et de données du Canada dans un marché sain et concurrentiel.
5. Participer à une initiative de stimulation économique afin d'inclure davantage d'entreprises et d'entrepreneurs du Canada dans l'économie numérique.
6. Adopter un rôle de leadership pour la création d'un cadre de représentant des données, en plus de développer, de commercialiser et d'exporter des produits et des services pour appuyer cette nouvelle industrie numérique.
7. Établir un cadre de gouvernance fédéral pour les fiduciaires de données.

Protection de la vie privée et confiance

1. Élaborer un cadre législatif national de consentement à l'utilisation des données afin de protéger les droits de chacun en matière de collecte et d'utilisation des renseignements personnels, ainsi que de préciser les différences entre la LPRPDE et la réglementation provinciale en matière de protection de la vie privée.
2. Revoir la *Loi sur la protection des renseignements personnels numériques* pour en faire une loi évolutive et agile par l'intermédiaire de mécanismes réglementaires qui peuvent être rapidement mis à jour afin d'évoluer au fil de la technologie, des cybermenaces et de la confidentialité exigée par la population canadienne.
3. Former une équipe d'intervention et de préparation aux atteintes à la protection des données composée de plusieurs intervenants de l'industrie, et assurer le déploiement d'un effort concerté entre les organismes d'application de la loi, les organismes de renseignement, les organisations de cybersécurité et les organisations de gestion numérique des données.
4. Mettre sur pied un organisme de réglementation au Canada responsable de la gestion des plaintes en matière d'atteinte à la protection des données et de la vérification des atteintes à la

protection des données signalées. Cet organisme devra disposer de pouvoirs en matière d'application de la loi et pouvoir imposer des mesures punitives lorsque les mesures de protection des données sont inadéquates. Cette entité devra se munir d'un protocole d'intervention rapide pour les incidents d'atteinte à la protection des données stratégiques et à grande échelle.

5. Établir un organisme de réglementation dont les responsabilités sont les suivantes.
 - a. Élaborer, mettre en œuvre et gérer des normes nationales en matière de protection des données.
 - b. Promouvoir la réglementation en matière de portabilité des données et la faire respecter. Les Canadiens devraient avoir le droit de fermer leur compte auprès d'une entreprise et de transférer leurs données ailleurs.
 - c. Permettre et simplifier le droit à l'oubli pour les jeunes de moins de 18 ans, ainsi qu'une réponse adéquate aux personnes de 18 ans et plus, déterminée en fonction de chaque cas.
 - d. Harmoniser les lois fédérales et provinciales en matière de protection des renseignements personnels des employés. Cette initiative devrait être jumelée à une campagne de sensibilisation tactique, propre à l'industrie et destinée au secteur privé afin d'énoncer les conséquences de la conformité du RGPD à la réglementation sur la protection des renseignements personnels des employés.

L'avenir du travail et les renseignements sur le marché du travail

1. Élaborer un cadre souple conçu pour saisir de façon exacte et opportune les réalités de l'industrie et en matière d'emploi dans le cadre des systèmes de CNP et de SCIAN, ce qui permettrait de saisir les plus récents développements à l'échelle de l'économie numérique, autant en ce qui concerne les secteurs prometteurs que les professions recherchées. Les processus de modification pertinents pourraient comprendre la séparation des sous-industries et des sous-professions des groupes élargies de la CNP et du SCIAN à des fins de granularité accrue. Le gouvernement du Canada et le secteur privé ont besoin de données plus exactes et granulaires sur les tendances en matière de renseignements sur le marché du travail afin de soutenir le secteur privé au moyen de politiques propres aux secteurs et de rivaliser à l'échelle internationale pour obtenir des investissements étrangers directs.
2. Traiter des enjeux en matière de suppression des données liés au système de CNP et au SCIAN de façon à fournir davantage de données importantes, exactes et granulaires, tout en tenant compte des besoins en matière de protection des données et de la vie privée. L'une des solutions potentielles consisterait à abaisser le niveau de suppression des données de l'actuel échantillon de 1 500 à 1 000 ou moins. À ce niveau, il serait non seulement possible de présenter des données fiables à l'échelle régionale et municipale, un aspect qui gagne en importance au fil de la conceptualisation des villes intelligentes, mais cela permettrait également de s'harmoniser plus étroitement avec les normes en matière de suppression des données des chefs de file comme l'OCDE. Par ailleurs, permettre l'accès aux microdonnées à des fins précises de recherche statistique (par exemple, fournir des prévisions exactes et agrégées en matière d'emploi à l'échelle régionale ou municipale) pourrait s'avérer une option intéressante.

3. Adopter un rôle de leadership mondial pour l'avenir du travail dans l'économie numérique en collaborant avec le secteur privé, les OSBL et les organisations de gestion des accréditations telles que Comptables professionnels agréés du Canada et Ingénieurs Canada afin d'établir une plateforme de microaccréditation viable et fiable.

Travaux cités

- Abrams, F. (2018, mai 7). *When 2 + 2 Might Equal 5*. Récupéré sur The New York Times: <https://www.nytimes.com/2018/05/07/opinion/google-right-to-be-forgotten-first-amendment.html>
- Anna Scott, A. D. (2018, octobre 05). *'agile ethics', how innovative organisations can adopt them and why diversity is so important to ethics*. Récupéré sur Open Data Institute: <https://theodi.org/article/agile-ethics-pioneer-alix-dunn-on-how-to-minimise-harm-and-why-moving-fast-and-breaking-things-must-not-extend-to-ethics/>
- Berinato, S. (2018). Stop Thinking About Consent: It Isn't Possible and It Isn't Right. *Harvard Business Review*. Récupéré sur Harvard Business Review: <https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right>
- Boyd, A. (2018, octobre 9). *East vs West in a race for AI supremacy*. Récupéré sur Asia Times: <http://www.atimes.com/article/east-vs-west-in-a-race-for-ai-supremacy/>
- Commission européenne. (2018, octobre 10). *Extending ESCO*. Récupéré sur Commission européenne: https://ec.europa.eu/esco/portal/escopedia/Extending_ESCO
- Connley, C. (2018, octobre 8). *Google, Apple and 12 other companies that no longer require employees to have a college degree*. Récupéré sur CNBC: https://www.cnbc.com/2018/08/16/15-companies-that-no-longer-require-employees-to-have-a-college-degree.html?__source=facebook%7Cmain
- Dunn, A. (2018, mai 7). *Working Ethically At Speed*. Récupéré sur Medium: <https://medium.com/@alixtrot/working-ethically-at-speed-4534358e7eed>
- École de la fonction publique du Canada. (2018, septembre 12). *Le Nuage de talents du GC*. Récupéré sur École de la fonction publique du Canada: <https://www.csps-efpc.gc.ca/events/gctc/index-fra.aspx>
- Edelman. (2018). *The 2018 Edelman Trust Barometer*. New York: Edelman.
- ENCQOR. (2018, 10 10). *ENCQOR*. Récupéré sur ENCQOR: <https://www.encqor.ca/>
- Eric Auchard, S. N. (2018, 03 15). *What is 5G and who are the major players?* Récupéré sur Reuters: <https://www.reuters.com/article/us-qualcomm-m-a-broadcom-5g/what-is-5g-and-who-are-the-major-players-idUSKCN1GR1IN>
- ESCO. (2018, octobre 10). *Extending ESCO*. Récupéré sur Classification européenne des aptitudes/compétences, certifications et professions: <https://ec.europa.eu/esco/portal?resetLanguage=true&newLanguage=fr>
- États-Unis, Mexique, Canada. (s.d.). *Chapter 19: Digital Trade*. Récupéré sur Office of the U.S. Trade Representative.
- Gouvernement du Canada. (2018, octobre 10). *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*. Récupéré sur Commissariat à la protection de la vie privée

du Canada: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/>

Gouvernement du Canada. (2018, octobre 10). *Loi sur la protection des renseignements personnels numériques*. Récupéré sur Site Web de la législation (Justice): https://laws-lois.justice.gc.ca/fra/LoisAnnuelles/2015_32/page-1.html

McConnell, J. (2018, janvier 31). *The digital economy has created a demand for 216,000 more tech workers, report finds*. Récupéré sur Financial Post: <https://business.financialpost.com/technology/the-digital-economy-has-created-a-demand-for-216000-more-tech-workers-report-finds>

NERC. (sans date). *Home Page*. Récupéré sur North American Electric Reliability Corporation: <https://www.nerc.com/Pages/default.aspx>

PWC UK, Open Data Institute. (2018, octobre 10). *The future of banking is open*. Récupéré sur pwc uk: <https://www.pwc.co.uk/openbanking>

Russell, A. (2018, octobre 31). *Canadians have little ability to determine if StatCan has their personal banking info: experts*. Récupéré sur Global News: <https://globalnews.ca/news/4615618/canadians-have-little-ability-to-determine-if-statcan-has-their-personal-banking-info-experts/>

Shecter, B. (2018, février 27). *Federal budget: Ottawa to study merits of 'open banking,' a catalyst for fintech*. Récupéré sur Financial Post: <https://business.financialpost.com/news/fp-street/ottawa-to-study-merits-of-open-banking-a-catalyst-for-fintech>

Statistique Canada. (2018, octobre 10). *Enquête sur la population active*. Récupéré sur Statistique Canada: <https://www.statcan.gc.ca/eng/survey/household/3701#a2>

The Canadian Press. (2018, 09 28). *Internet groups disappointed in lowered CRTC speed minimums for broadband fund*. Récupéré sur Financial Post: <https://business.financialpost.com/pmn/business-pmn/internet-groups-disappointed-in-lowered-crtc-speed-minimums-for-broadband-fund>

Union européenne. (2018, octobre 10). Récupéré sur EUR-Lex - L'accès au droit de l'Union européenne: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>

Union européenne. (2018, octobre 10). Récupéré sur EUR-Lex - L'accès au droit de l'Union européenne: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>

Union européenne. (2018, octobre 10). Récupéré sur EUR-Lex - L'accès au droit de l'Union européenne: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>

Union européenne. (2018, octobre 10). Récupéré sur EUR-Lex - L'accès au droit de l'Union européenne: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:02016R0679-20160504&from=EN>

