Feuille de route du Collectif canadien de normalisation en matière de gouvernance des données

Conseil canadien des normes

Un monde de possibilités à votre portée.

Canada

Table des matières

Remerciements

Nous remercions sincèrement toutes les personnes et organisations (voir l'annexe E) qui ont fourni leur avis technique ou leur aide pour l'élaboration de la présente feuille de route. Ce document n'aurait pu voir le jour sans leur engagement, leur implication et leur contribution tout au long de la dernière année.

La feuille de route repose sur un consensus entre les personnes et les organisations qui ont activement participé à son élaboration et ne reflète pas nécessairement le point de vue individuel de chacune d'elles.

Par ailleurs, nous souhaitons remercier sincèrement l'American National Standards Institute (ANSI), notamment Jim McCabe, le directeur principal de la promotion des normes. La feuille de route est basée sur la méthodologie et les mécanismes mis en place par l'organisme au cours des 15 dernières années. Pour en savoir davantage sur les collectifs de normalisation de l'ANSI, visitez son site Web : https://www.ansi.org/standards-coordination/coordination-us-system.

Cette initiative a été financée par le Conseil canadien des normes dans le cadre du Plan pour l'innovation et les compétences du Canada afin d'aider directement les innovateurs canadiens à se servir du système de normalisation comme moteur de croissance et de compétitivité.

Message des coprésidents du comité directeur du Collectif canadien de normalisation en matière de gouvernance des données

Créé en 2019, le Collectif canadien de normalisation en matière de gouvernance des données est l'un des premiers projets réalisés dans la foulée du lancement de la Charte canadienne du numérique. À sa formation, nous avions pour ambition de concevoir une feuille de route sur la normalisation avant la fin de 2020. Nous ignorions alors les bouleversements que le monde s'apprêtait à connaître – et la rapidité avec laquelle les normes se révéleraient fort utiles pour traverser cette épreuve.

Les défis de la pandémie de COVID-19 ont accéléré des transitions fondamentales dans nos sociétés et nos économies. De nos jours, les données – provenant de sources plus nombreuses que jamais – sont en constante circulation. Il est donc crucial de se doter d'un langage commun pour leur partage.

Essentielles à la collaboration, les normes servent de pont pour communiquer des idées entre les individus, les secteurs et les nations, et même entre les époques. Elles catalysent l'innovation, en assurant un travail colossal d'intégration des données et le maintien de l'interopérabilité des systèmes, ce qui permet aux innovateurs de se concentrer sur les découvertes et les inventions. Elles sont reconnues comme une méthode agile pour adapter les lois fondées sur des principes à des secteurs et des technologies en particulier, et comme un outil de promotion des efforts de conformité à venir. La pandémie nous a donné un exemple remarquable de leur mise en application : elles ont en effet contribué à mettre en branle un partage de données sans précédent partout dans le monde, menant à la mise au point de vaccins contre la COVID-19 en un temps record.

Dans la dernière année, le Collectif a également travaillé d'arrache-pied pour cerner les secteurs de collaboration et d'innovation potentiels. Nos groupes de travail se sont rencontrés virtuellement pour discuter d'études de cas constituant des exemples pragmatiques des principales questions d'actualité concernant la gouvernance des données. Une étude s'est penchée sur les failles des données dans notre système de santé. Une autre s'est attelée aux finances axées sur les clients, mieux connues sous le nom de « système bancaire ouvert ». Une troisième a examiné le trajet de la nourriture du champ à l'assiette dans le cadre de la transformation numérique de la chaîne d'approvisionnement de l'alimentation. Nous remercions les groupes de travail – qui ont dû trier des centaines d'enjeux de normalisation pour arriver aux trente-cinq recommandations qui se trouvent dans cette première version de la feuille de route – pour le temps et la réflexion consacrés à la cartographie du paysage normatif.

Pour faire progresser ces recommandations, nous devons maintenant construire la base du pont. La confiance en l'économie numérique sera essentielle pour protéger la santé, la sécurité et le bien-être de la population. Dans son travail sur les enjeux de gouvernance des données, notre Collectif continuera de sensibiliser les décideurs aux façons de susciter la confiance chez le public et de protéger la confidentialité et la sécurité des Canadiens.

Nous voulons remercier nos membres pour leur collaboration, leur confiance mutuelle et leur volonté de faire avancer notre travail au profit de l'ensemble de la population. Nous souhaitons également exprimer notre reconnaissance à notre organisme fondateur, le Conseil canadien des normes, pour son soutien et ses conseils.

Anil Arora, statisticien en chef du Canada

Philip Dawson, conseiller principal des politiques, Responsible AI Institute

Message de la directrice générale du Conseil canadien des normes

Le traitement et la gestion des données ont des effets à long terme sur la santé, le bien-être et la prospérité des Canadiens. Une occasion exceptionnelle nous est offerte de tirer parti des données et de mieux les utiliser pour stimuler la croissance et protéger la population. D'après la Charte canadienne du numérique, la normalisation contribuera à soutenir l'innovation et aidera les entreprises canadiennes à rester concurrentielles à l'international.

Le Conseil canadien des normes (CCN) a créé le Collectif canadien de normalisation en matière de gouvernance des données pour coordonner les stratégies de normalisation de la gouvernance des données d'un océan à l'autre. Notre plan de travail est de grande envergure. Au cours de la dernière année, nous avons collaboré avec plus de 220 Canadiens du gouvernement, de l'industrie, de la société civile, d'organisations autochtones, d'universités et d'organismes d'élaboration de normes afin d'examiner de près l'encadrement normatif de la gouvernance des données au pays : l'état des lieux et les défis actuels, et l'avenir idéal.

Notre feuille de route décrit les principaux enjeux liés à la gouvernance des données, relève les lacunes dans la normalisation et fournit des recommandations pour les combler. Elle vise à nous guider dans un moment crucial de l'histoire et nous permettra de nous attaquer aux questions difficiles entourant l'avenir et la planification de la gouvernance des données au pays.

Mener à terme la feuille de route en pandémie n'a pas été une mince tâche. Je suis encore impressionnée par l'ardeur dont chacun des participants a fait preuve. La force du Collectif réside dans la diversité des gens qui lui ont consacré temps et énergie.

Bien appliquée, la normalisation souligne et promeut l'excellence; elle vise à libérer le potentiel pour faire en sorte que les Canadiens aient accès aux produits, aux systèmes et aux solutions technologiques les plus sûrs au monde.

Au cours des prochaines années, le CCN, en étroite collaboration avec des organismes d'élaboration de normes et d'autres partenaires clés, cherchera à mettre en œuvre la présente feuille de route et ses 35 recommandations. Nous dirigerons ce travail en faisant ce que nous faisons le mieux : aider à résoudre des problèmes complexes en rassemblant les parties intéressées et le réseau de la normalisation dans la création commune des stratégies et des solutions nécessaires pour protéger la santé et la sécurité de la population.

Chantal Guay

Chantal Guay, ing. FACG

Sommaire

En 2019, dans la foulée du lancement de son plan d'action, la Charte canadienne du numérique reconnaissait que les normes et l'évaluation de la conformité constituaient des outils importants pour « encourager l'élaboration et la mise en œuvre de nouveaux mécanismes de gouvernance des données. » Elle stipule que le Canada a « la possibilité d'être proactif et de prendre un rôle de chef de file dans des domaines émergents de la gestion du numérique et des données, aidant ainsi à établir des repères ou des normes mondiales [et que de] **permettre des certifications et normalisations au niveau international pourrait apporter des certitudes à ces marchés perturbateurs et permettre au Canada de participer à l'élaboration de normes mondiales**[1]. »

En novembre 2020, le gouvernement a proposé la *Loi de 2020 sur la mise en œuvre de la Charte du numérique* dans le but d'élaborer une stratégie nationale visant à tirer les avantages économiques des données tout en atténuant les méfaits possibles. Au même moment, le Conseil sur la stratégie industrielle publiait un plan de croissance ambitieux pour bâtir une économie numérique, durable et innovante, qui souligne la nécessité de recourir aux normes et à l'évaluation de la conformité (la normalisation), des rouages essentiels à la transformation du Canada en **une économie numérique et axée sur les données**[2].

Le Collectif canadien de normalisation en matière de gouvernance des données (CCNGD ou « le Collectif ») a été formé en réponse à la Charte du numérique **pour coordonner l'élaboration et la compatibilité des normes sur la gouvernance des données et des programmes complémentaires d'évaluation de la conformité au pays, contribuant à l'économie numérique et axée sur les données**. Premier produit du Collectif, cette feuille de route consacrée à la chaîne des valeurs de la gouvernance des données décrit le paysage normatif actuel et souhaité au pays; elle comprend des recommandations pour combler les lacunes et pointe les nouveaux secteurs où le Canada peut s'ériger en chef de file de l'élaboration des normes et en agent de changement à l'international dans la sphère de la gouvernance des données et des mégadonnées.

Basés sur les 35 recommandations du Collectif soulignant **l'importance de disposer de solutions de normalisation de la gouvernance des données axées sur les besoins opérationnels et stratégiques, trois grands thèmes** se dégagent de cette feuille de route :

1. **Qualité** – mise en œuvre de solutions de normalisation pour les systèmes et les mesures de contrôle visant l'obtention de données de grande qualité.
2. **Confiance** – établissement d'un climat de confiance par la normalisation pour garantir une bonne utilisation des données, dans le respect de la vie privée, de la sécurité et de la réglementation et des cadres de transparence.
3. **Éthique** – mise en place d'outils d'IA et d'apprentissage machine éthiques, et dont l'explicabilité (propriété d'être compris par des humains) est assurée par la normalisation, les systèmes et d'autres mesures de contrôle.

Grâce à des solutions de normalisation, nous aurons des données de meilleure qualité et des mécanismes d'accès fiables, et les outils déployés seront éthiques, honnêtes et licites.

Le rapport s'appuie sur les recommandations de la Charte du numérique et **met en action la normalisation**, catalyseur de changements et solution de relance post-pandémie. La feuille de route trace un cadre pour des conversations et des interactions utiles, fiables et transparentes entre les gouvernements, les gouvernements et organisations autochtones, les industries, la société civile, les organismes de normalisation et les citoyens canadiens.

1 La Charte numérique du Canada en action : un plan par les Canadiens, pour les Canadiens. https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00109.html.

2 « L'économie numérique, c'est l'activité économique qui découle de milliards de connexions en ligne quotidienne entre individus, entreprises, appareils, données et processus. Au cœur de cette dernière se trouve l'hyperconnectivité, soit l'interconnexion croissante entre individus, organisations et machines, fruit de l'Internet, des technologies mobiles et de l'Internet des objets. » https://www2.deloitte.com/mt/en/pages/technology/articles/mt-what-is-digital-economy.html. Une économie est dite axée sur les données lorsque les données sont utilisées pour améliorer les processus, produits, méthodes organisationnelles et marchés sociaux et économiques. « L'économie axée sur les données, tout comme l'économie du savoir d'où elle tire son origine, présente des économies d'échelle et des externalités de réseau, ce qui donne lieu à des structures de marché concentrées, un accroissement du loyer du marché et des mesures visant à inciter les comportements stratégiques, y compris dans les politiques commerciales. » https://www.cigionline.org/articles/economics-data-implications-data-driven-economy#:~:text=In%20terms%20of%20market%20structure,including%20in%20trade%20policy%20(as.

La normalisation est un outil bien connu dans les secteurs traditionnels. Intégrée à nos codes du bâtiment et à nos règlements, elle nous protège discrètement lors de la construction de nos infrastructures sans que nous ayons à y réfléchir. Nous sommes entrés dans une époque où les gens, les organismes et les communautés utilisent une infrastructure intangible (Internet) ou interagissent avec elle. Or, les règles de gouvernance, notamment celles sur la confidentialité et la sécurité des données, en sont encore à leurs balbutiements. La normalisation (et tout ce qu'elle suppose) reconnaît le besoin de changement et d'amélioration continus (des normes, des services, des produits, etc.) et adopte une approche globale de la vérification et de la conformité pour suivre l'évolution des enjeux stratégiques et opérationnels de la gouvernance des données.

Cette feuille de route ouvre la voie à une discussion fructueuse sur la mise en œuvre, par la normalisation, des divers éléments qui composent la gouvernance des données au Canada. En plus de ces implications stratégiques globales, la feuille de route présente des recommandations concrètes à mettre en place dans les cinq prochaines années pour avoir le plus de retombées tout en utilisant les ressources de manière efficace.

Saisissez cette occasion de **PASSER À L'ACTION** :

- Partenaires gouvernementaux, cette feuille de route vous aidera à comprendre comment la participation à l'élaboration de solutions de normalisation faciliterait la préparation de politiques publiques, notamment par l'incorporation par renvoi dans les règlements et l'utilisation de programmes nationaux d'évaluation de la conformité pour appuyer des accords commerciaux internes et externes;
- Partenaires de normalisation, cette feuille de route appuiera l'élaboration de nouvelles solutions de normalisation nécessaires; les enjeux qui y sont présentés ont été sélectionnés de façon à entreprendre ou à poursuivre l'élaboration de solutions de normalisation qui permettraient de combler des lacunes cernées, et ériger le Canada en chef de file de l'élaboration de normes nationales et internationales et de programmes d'évaluation de la conformité pour la gouvernance des données;
- Partenaires du secteur privé, cette feuille de route vous aidera à mieux comprendre comment les outils de normalisation peuvent aider les entreprises à percer de nouveaux marchés, à croître pour ouvrir un marché, à respecter les nouveaux règlements et à naviguer dans le système de normalisation (surtout pour les PME aux ressources limitées);
- Partenaires d'organisations de la société civile, cette feuille de route met en lumière la nécessité d'une meilleure gouvernance des données dans la société civile et de montrer l'exemple en offrant « une autre voie que le modèle débridé d'exploitation des données à grande échelle de plusieurs grandes entreprises de technologie[3]. »
- Citoyens canadiens, cette feuille de route vous aidera à comprendre comment la normalisation, un outil qui s'intègre déjà naturellement à votre quotidien, aidera à construire des infrastructures numériques plus sûres et mieux sécurisées fondées sur la qualité, la confiance et l'éthique pour la santé et la sécurité de la population, alors que de plus en plus de services et de transactions sont virtuels.

Un dernier point et non le moindre, sur lequel repose la **valeur et la fondation du Collectif : ce travail ne peut s'accomplir sans collaboration entre *toutes* les parties prenantes**. Pour que le pays et la population puissent profiter d'une économie numérique et axée sur les données, les outils de normalisation devront agir comme catalyseur pour :

- tabler sur des solutions numériques des secteurs privé et, public et de la société civile pour améliorer la qualité des infrastructures de données, les simplifier et les moderniser;
- promouvoir le partage de données produites par des organisations privées, publiques et de la société civile entre de multiples intervenants de divers secteurs sur des plateformes ou portails fiables;
- donner plus de contrôle et de pouvoir décisionnel aux propriétaires de données sur le partage et l'utilisation éthique de leurs données pour répondre à des questions de fond communes.

Si vous avez besoin de plus amples renseignements sur l'utilisation de cette feuille de route ou sur les façons d'y contribuer, communiquez avec le Conseil canadien des normes à l'adresse info@ccn.ca.

3 Open Society Foundations, *Civil Society Organizations and General Data Protection Regulation Compliance*, 2020

Utilisation du rapport

Normes et évaluation de la conformité

Une norme est un document qui fournit des règles, des lignes directrices ou des caractéristiques convenues pour des activités ou leurs résultats. Les normes définissent les pratiques acceptables, les exigences techniques et la terminologie utilisée dans divers domaines. D'application obligatoire ou facultative, elles se distinguent des lois, des règlements et des codes, mais peuvent néanmoins être citées dans ces documents juridiques (voir les *Lignes directrices sur l'incorporation par renvoi de normes dans la réglementation en appui aux objectifs de politiques publiques*[4]).

L'évaluation de la conformité est la pratique qui consiste à déterminer si un produit, un service ou un système répond aux exigences d'une norme donnée.

La normalisation est l'élaboration et l'application de normes : le travail des comités d'élaboration; la publication par des organismes d'élaboration de normes; la reconnaissance par des organismes nationaux de normalisation comme le CCN; l'application par les entreprises, les fournisseurs et les clients, la vérification de la conformité de produits ou de services aux normes applicables (évaluation de la conformité); l'accréditation d'organisations offrant des services d'évaluation de la conformité; et l'intégration de normes et d'évaluations de la conformité aux politiques publiques ainsi qu'au commerce international.

Le CCN est le représentant du Canada en matière de normalisation et d'accréditation sur les scènes nationale et internationale. Il collabore de près avec un vaste réseau de partenaires pour encourager l'élaboration de normes efficientes et efficaces qui favorisent la santé, la sécurité et le bien-être de la population canadienne, ainsi que la prospérité des entreprises. Principal organisme d'accréditation du Canada, le CCN renforce la confiance des marchés au pays et à l'étranger en veillant à ce que les organismes d'évaluation de la conformité respectent les normes nationales et internationales les plus strictes. En tant que membre de l'Organisation internationale de normalisation (ISO) et de la Commission électrotechnique internationale (IEC), le CCN défend les intérêts du Canada sur la scène internationale et met en contact des milliers de personnes avec des réseaux et des ressources du monde entier. Par son action, il ouvre une porte sur un monde de possibilités pour les Canadiens et les entreprises.

4 https://www.scc.ca/fr/notre-organisme/publications/documents-de-politique/lignes-directrices-sur-lincorporation-par-renvoi-de-normes-dans-la-reglementation-en-appui-aux

Le Collectif

Fondé en 2019, le Collectif canadien de normalisation en matière de gouvernance des données rassemblait plus de 220 acteurs canadiens de l'industrie, des gouvernements, de la société civile, du milieu de la recherche et des organismes d'élaboration de normes (OEN). Il avait pour tâche d'élaborer une feuille de route cohérente sur les normes en vigueur et nécessaires en matière de gouvernance des données et de fournir des recommandations applicables sur les modes d'utilisation possibles des codes de pratique, de la certification et des normes pour transposer des lois fondées sur des principes à des secteurs, activités ou technologies en particulier, et faire en sorte que les cadres gagnent en flexibilité et inspirent davantage confiance à la population canadienne.

Pour parvenir à une représentation équilibrée des principaux groupes actifs dans la sphère de la gouvernance des données, l'ensemble des intervenants du pays ont été invités à participer à cet effort, qu'ils fassent ou non partie du système de normalisation volontaire supervisé par le CCN. Parmi les secteurs représentés dans le Collectif, mentionnons l'aérospatiale, les communications, la construction, les technologies numériques, l'électronique, l'énergie, les services financiers, la santé, l'agriculture et l'agroalimentaire, les services publics et le commerce de détail.

Les membres du Collectif qui ont travaillé sur la feuille de route se sont attaqués à certaines questions difficiles concernant la normalisation et la gouvernance des données. Le Collectif tire sa force de la grande diversité des personnes[5] qui ont consacré temps et énergie à ce projet.

Lecture de la feuille de route

La feuille de route s'adresse à un public vaste : le gouvernement du Canada, en appui à la Charte canadienne du numérique et à la gouvernance des données en général; les organismes de normalisation qui cherchent à orienter l'élaboration de normes et leur stratégie en matière de gouvernance des données; les administrations provinciales, territoriales et municipales; les organismes de réglementation; les organismes législatifs et réglementaires; les industries; le milieu de la recherche; et le public qui cherche à connaître les stratégies et les activités de normalisations mises en place pour encadrer la gouvernance des données dans toute sa complexité.

Visant à orienter le débat sur des questions d'actualité cruciales qui auront des conséquences à long terme, cet outil est conçu pour guider l'allocation des ressources destinées aux intervenants qui participent à la planification et à l'élaboration des normes et aux activités de recherche et développement qui y sont rattachées (dans la mesure où elles sont nécessaires). Le document s'adresse aux acteurs directement touchés par la gouvernance des données qui comprennent les principaux enjeux qui y sont liés.

La feuille de route est principalement le reflet de l'expertise de ceux qui ont œuvré à son élaboration. Sa portée peut sembler vertigineuse de prime abord, ce qui est exactement l'impression donnée par le terme « gouvernance des données » lorsqu'on l'appréhende dans sa complexité. Nous savons tous que le traitement et la gestion des données ont des répercussions sur l'ensemble de notre économie. Des finances à la santé, de l'éducation aux loisirs, de la fabrication à la vente au détail : la production, l'analyse et l'utilisation des données touchent tous les aspects de nos vies. L'absence de normes claires et de programmes d'évaluation de la conformité visant à promouvoir une utilisation adéquate des données compromet la vie privée des citoyens et la compétitivité de notre économie.

La première section de la feuille de route décrit le contexte stratégique de la normalisation et de la gouvernance des données au Canada. Elle présente des cas d'usage qui montrent la façon dont les divers secteurs de l'économie numérique, nouveaux ou traditionnels, composent avec un régime complexe de gouvernance des données et ses répercussions sur l'économie, la concurrence et surtout la sécurité. Elle fait état des résultats de la consultation autochtone sur ces enjeux, non pas par un simple résumé des points de vue autochtones sur la question, mais plutôt en soulignant la nécessité de mobiliser les groupes autochtones pendant l'ensemble du processus pour qu'ils puissent contribuer davantage à l'élaboration et à l'application de normes ou d'initiatives de gouvernance des données au Canada.

5 Les femmes représentaient 41 % des membres du Collectif

La deuxième section présente les grandes lignes des 35 principaux enjeux étudiés par le Collectif et des recommandations qui en découlent. Elle traite notamment de la portée de ces enjeux, des besoins définis et des exemples de leur effet sur les individus et les organisations, et met en lumière l'incidence de l'intangible de la gouvernance des données sur des aspects concrets de notre existence. On y trouvera les 35 recommandations générales qui forment un plan d'action pour un véritable cadre canadien de gouvernance des données.

La troisième section résume les recommandations et les prochaines étapes qui permettront de passer de la théorie à la pratique par la mise en œuvre de normes et la réponse aux besoins connexes en matière d'évaluation de la conformité.

Les annexes, qui présentent en détail les travaux du Collectif, contiennent de l'information utile à ceux qui souhaitent connaître des renseignements précis ou la méthodologie utilisée pour l'élaboration de la feuille de route : analyses des groupes de travail (annexes A et B), rapport complet sur la consultation autochtone (annexe C), rapports sur les cas d'usage (annexe D), liste des membres du Collectif (annexe E), liste des acronymes et abréviations (annexe F), méthode d'élaboration du paysage normatif par le Collectif (annexe G), brève description des OEN et autres entités en gouvernance des données (annexe H) et paysage normatif détaillé (annexe I).

Normalisation et gouvernance des données au Canada

État des lieux

Concept très vaste, la gouvernance des données découle de la gestion de l'information, et se concentre essentiellement sur les pratiques exemplaires de collecte, de stockage, d'archivage et d'élimination des données. Elle comprend en effet les volets de collecte, de protection de la vie privée, d'utilisation, de synthèse et d'analyse, de contrôle, de publication, de stockage et d'archivage et d'élimination. Or depuis l'avènement de l'Internet au début des années 1990, ces notions et leurs implications pour les individus, les organisations et les communautés revêtent désormais une tout autre dimension.

De même, les concepts de vie privée et d'accès à l'information découlant de l'évolution rapide de l'intelligence artificielle et de l'apprentissage machine ainsi que d'appareils et de capteurs connectés à l'Internet des objets ont poussé de nombreux pays à se doter rapidement de stratégies sur les données pour dénouer la tension entre leur statut de « ressource » nationale et les préoccupations d'éthique et de confidentialité pour les individus, les organisations et les communautés. Le Canada ne fait pas exception, car malgré la renommée de ses innovateurs et de leurs créations, il n'en demeure pas moins que dans un monde où l'économie accorde une place grandissante aux données, il accuse un retard[6].

En mai 2019, Innovation, Sciences et Développement économique Canada (ISDE) lançait la Charte canadienne du numérique : La confiance dans un monde numérique. Reposant sur dix principes, ce projet a permis « d'orienter le travail du gouvernement fédéral, en servant de charte du numérique pour les Canadiens qui aidera à relever les défis tout en exploitant les talents et les points forts uniques du Canada afin d'utiliser le pouvoir de la transformation du numérique et des données[7]. » D'après cette charte, la normalisation contribuera tout particulièrement à soutenir l'écosystème d'innovation et aidera les entreprises canadiennes à rester concurrentielles à l'international.

C'est dans la foulée de ce lancement, à l'été 2019, que le Collectif canadien de normalisation en matière de gouvernance des données, un organe de coordination intersectoriel, a été fondé dans le but d'accélérer, à l'échelle de l'industrie, l'élaboration de normes et de spécifications qui répondent aux besoins des intervenants et catalysent la croissance des capacités en matière de gouvernance des données en fonction des priorités nationales et mondiales.

6 https://ppforum.ca/fr/publications/deux-pics-a-franchie-les-deux-deficits-du-canada-et-comment-les-proportionner/
7 https://www.ic.gc.ca/eic/site/062.nsf/fra/h_00109.html

Compte tenu de l'existence de processus parallèles sur la gouvernance des données sans lien avec la normalisation volontaire, le Collectif avait les objectifs suivants :

- L'établissement et la définition d'axes prioritaires canadiens de gouvernance des données susceptibles de tirer profit de la normalisation.
- La production d'une feuille de route exhaustive décrivant le paysage normatif actuel et souhaité de la gouvernance des données au Canada, et recommandant des mesures pour combler les lacunes et répondre aux besoins en matière de normalisation et d'évaluation de la conformité dans de nouveaux domaines.
- La formulation de recommandations en matière d'initiatives de normalisation, de calendriers et d'organismes compétents, tant à l'échelle nationale qu'internationale.

Les activités du Collectif ont été regroupées sous quatre grands thèmes (groupes de travail) inspirés du modèle du cycle de vie et de la chaîne des valeurs des données : 1) Fondements de la gouvernance des données, 2) Collecte, organisation et classement, 3) Accès, diffusion et conservation, 4) Analyse, solutions et commercialisation. De ces thèmes, une liste de sujets généraux a été dressée en lien avec les normes et les programmes d'évaluation de la conformité sur la gouvernance des données.

Le Collectif reconnaît qu'un certain nombre d'organismes d'élaboration de normes ou d'organisations connexes – à l'échelle nationale, régionale et internationale – œuvrent à la production de normes volontaires et consensuelles pour un large éventail d'enjeux liés à la gouvernance des données en vue de répondre aux besoins de divers secteurs. L'existence de ces activités de normalisations parallèles ne fait que mettre en évidence la nécessité de se doter d'un leadership et d'une coordination à l'échelle nationale afin que les intervenants disposent toujours un jeu de normes cohérentes, harmonisées et non contradictoires concernant la gouvernance des données.

Les actifs incorporels comme l'analyse de données occupent aujourd'hui une place centrale dans le monde des technologies de l'information et des communications; aussi leur propriété et leur commercialisation ont profondément changé les modalités d'interaction des économies qui espèrent se tailler une place dans l'environnement technologique moderne. Les données étant désormais essentielles aux industries, et capitales pour le secteur en pleine expansion de l'intelligence artificielle, il faut adapter la gouvernance et les protocoles aux nouvelles réalités de l'analyse de données. Qui plus est, ces nouvelles avancées et ces nouveaux réseaux ont mis à l'épreuve les cadres réglementaires et les mécanismes de conformité qui en découlent (actuels et à venir).

Les organisations ont un rôle de plus en plus important dans la gestion des données qu'elles produisent, de même que dans le type d'analyses qu'elles mènent. D'ailleurs, le nombre d'entreprises se consacrant exclusivement aux ensembles de données externes et proposant des solutions d'analyse et de gestion ne cesse d'augmenter. Il faut tenir compte des besoins particuliers de secteurs comme ceux, fortement réglementés, de la santé et des finances, et de nouveaux besoins découlant de la croissance de secteurs traditionnels, notamment l'agriculture et l'assurance. Les entreprises de ces secteurs doivent non seulement voir à la gestion de leurs données dans leur structure, mais aussi à leur échange avec les autres entreprises et organisations.

Il faut également adapter les principes éthiques de gouvernance des données à la société civile et leur accorder une place définie dans les règlements, les pratiques exemplaires et les normes. Dans l'article *Information Ethics: Coalition building with Civil Society and Taking Responsibility for AI Evolution*[8], les auteures explorent le rôle de la société civile dans l'élaboration d'un cadre normatif. Elles avancent que « pour être représentatifs, les processus d'innovation réglementaires doivent permettre à la société civile de participer activement aux consultations sur l'innovation en matière de politiques. Les partenariats publics-privés doivent être transformés en partenariats publics-privés-civils ». L'exploitation des données personnelles et communautaires est maintenant couramment abordée, notamment dans le cadre de discussions sur le capitalisme de surveillance et l'érosion de l'autonomie et de la démocratie.

8 Goddard, Valentine et Myriam Côté, *Information Ethics: Coalition building with Civil Society and Taking Responsibility for AI Evolution*.

Étant donné la nature des données et la multiplication de leur circulation d'une organisation à l'autre, l'élaboration et l'adoption de normes sur la structure, la gouvernance et la sécurité des données s'imposent comme une nécessité. Les OEN se penchent depuis peu sur l'établissement de normes pour répondre aux besoins en la matière. Cet exercice de normalisation s'appuie sur d'anciennes exigences de normalisation en gestion de l'information, qu'on a adaptées à la réalité de la gestion de données en contexte d'automatisation industrielle. Outre les OEN, des consortiums dirigés par l'industrie et des plateformes à code source libre continuent de participer à la normalisation de l'information et des communications, et intègrent la question de la gouvernance des données.

La quantité considérable de normes visant à encadrer les stratégies numériques est préoccupante. Comment profiter de l'économie numérique sans hypothéquer la santé et la sécurité des gens, des organisations et des communautés lorsque la multiplicité des normes élaborées dans les forums de normalisation ouverte ou volontaire alimente la confusion plutôt que de la dissiper? Il faut que les gouvernements, l'industrie et la société civile réfléchissent et prennent le pouls du paysage normatif pour élaborer un cadre de gouvernance dont les normes sont la pierre angulaire.

Les pays et régions se penchent sur les stratégies de données et outils de normes et d'évaluation de la conformité à leur disposition pour appuyer les cadres de mesures sur les données. Par exemple, en septembre 2020, le Royaume-Uni a dévoilé sa stratégie nationale sur les données dans le but de « coopérer avec les nations pour élaborer des normes communes qui cadrent avec les intérêts et objectifs nationaux du pays, à savoir que les normes techniques sont appelées à exprimer des valeurs éthiques et sociales ainsi que des pratiques exemplaires.[9] »

En 2020, la Commission européenne a déposé une proposition de règlement sur la gouvernance européenne des données (acte sur la gouvernance des données), la première d'une série de mesures annoncées dans le cadre de la stratégie européenne de 2020. L'une des tâches énoncées dans la proposition consiste à « conseiller la Commission sur la hiérarchisation des normes transsectorielles à utiliser et à mettre au point pour l'utilisation de données et le partage de données entre différents secteurs, la comparaison et l'échange transsectoriels des meilleures pratiques en ce qui concerne les exigences sectorielles de sécurité, les procédures d'accès, tout en tenant compte des activités de normalisation transsectorielle [et à] aider la Commission à améliorer l'interopérabilité des données ainsi que les services de partage de données entre les différents secteurs et domaines, en tirant parti des normes européennes, internationales ou nationales existantes[10]. » En avril 2021, la Commission européenne a déposé une proposition de nouvelles règles visant à encadrer l'IA dans l'Union européenne, qui, dans leur formulation actuelle, accorderaient une plus grande place à la normalisation et à l'évaluation de la conformité pour protéger la santé, la sécurité et les droits fondamentaux dans la gestion et l'utilisation des données et de l'IA.

L'entrée en vigueur du *Règlement général sur la protection des données (RGPD)* a modernisé le paysage juridique de la confidentialité des données à l'échelle mondiale. Ainsi, les entreprises d'autres coins du monde ont rapidement compris, adopté et mis en œuvre les exigences et programmes en la matière pour pouvoir traiter avec l'UE. À cet égard, le CCN a publié un document d'orientation pour faire connaître le RGPD aux organisations canadiennes[11] qui recommande des stratégies de normalisation pour en faciliter le respect. Aux États-Unis, le National Institute of Normes and Technology (NIST) a également publié en 2020 une série de lignes directrices pour aider les entreprises du pays à s'adapter aux exigences toujours plus grandes en matière de confidentialité des données, *The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management*. Il s'agit d'un ensemble de procédures volontaires visant à aider les entreprises à comprendre les mesures d'observation des divers règlements sur la protection des données partout dans le monde.

9 https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy#fnref:23
10 https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:52020PC0767&from=EN.
11 https://www.scc.ca/fr/notre-organisme/publications/general/comprendre-le-rgpd-le-role-des-normes-dans-la-conformite.

Dans la dernière année, les données « ont été une bouée de sauvetage durant la pandémie mondiale de coronavirus[12], » et la normalisation à l'échelle régionale, nationale et internationale a permis d'optimiser l'utilisation de données pour l'innovation et le soutien de la croissance économique. Outil de politique publique, la normalisation vise aussi à résoudre des questions éthiques fondamentales touchant le partage, l'utilisation et la propriété des données, et leurs conséquences pour les individus et les communautés.

La COVID-19 a accéléré des virages fondamentaux dans notre société et notre économie. Dans un monde aux sources de données multiples où l'information circule constamment, il est crucial de se doter un langage commun pour l'échange de données. Au cœur de ce projet, les normes, essentielles à la collaboration, servent de pont pour communiquer des idées entre les individus, les secteurs et les nations, et même entre les époques. Sans les normes instaurées par les gouvernements, les chercheurs et les entreprises à l'origine de l'Internet, un tel échange d'idées n'aurait pu voir le jour. Non seulement les normes permettent la collaboration, mais elles accélèrent l'innovation. À preuve, le vaccin contre la COVID-19 : une innovation dont nous profitons tous.

Lors de la pandémie, les normes ont permis un partage de données sans précédent entre scientifiques des quatre coins du monde. Résultat? Un séquençage du nouveau coronavirus à peine quelques jours après sa découverte en Chine. Moins d'un an plus tard, les premiers vaccins étaient autorisés au Canada. C'est un record de vitesse, le précédent étant détenu par le vaccin contre les oreillons, développé en quatre années. Bien que la recherche ayant contribué au développement des vaccins contre la COVID-19 ait commencé plusieurs années auparavant, les efforts mondiaux de partage de données ont mené à des progrès rapides qui transformeront presque assurément l'avenir de la vaccinologie. Rien de tout cela n'aurait été possible sans normes permettant l'interopérabilité et l'intégration de systèmes de partage de l'information[13]. Sans elles, nous n'aurions pas de langage commun pour faire progresser les connaissances issues de la recherche.

Relever les défis et repérer les occasions

Les groupes de travail du Collectif se sont réunis virtuellement une douzaine de fois pour travailler ensemble sur les principaux enjeux de gouvernance des données et des études de cas d'usage, des exemples pratiques invitant à la réflexion sur la gouvernance des données.

Grâce à leur travail crucial pour cibler les secteurs où des normes existent déjà, nous pouvons puiser dans notre arsenal pour commencer à trouver des solutions. Certaines normes internationales sont adaptables au contexte canadien, mais d'autres nécessiteront un leadership réel du Canada pour que le pays définisse les normes et soit un chef de file de l'élaboration de programmes d'évaluation de la conformité qui puissent servir de base pour de futurs programmes internationaux d'accréditation encadrant les échanges mondiaux dans l'économie de l'immatériel. Par exemple, le CCN, aidé et financé par ISDE, facilite l'élaboration de documents à caractère normatif dans un projet sur les identifiants numériques. Il présentera des critères d'évaluation de la conformité et un programme d'accréditation pour faire progresser cette initiative et la tester auprès d'autorités de réglementation, d'entreprises et d'organismes d'évaluation de la conformité nationaux.

Pour favoriser l'adoption des recommandations de la présente feuille de route, nous devons insuffler une confiance envers les ententes qui régissent le partage de données entre les groupes des gouvernements, de l'industrie et de la société civile. Dans notre confédération au pouvoir décentralisé et délégué aux provinces et territoires s'applique une mosaïque de règlements. Une norme fait ici office de « loi » souple, plus digeste et facile à respecter, applicable d'une province et à d'un territoire à l'autre. Il importe que le Collectif poursuive le dialogue avec les décideurs, l'industrie et la société civile sur les façons de favoriser la confiance du public et de protéger la vie privée des Canadiens.

12 http://data.parliament.uk/DepositedPapers/Files/DEP2020-0521/UK_National_Data_Strategy.pdf.
13 https://www.who.int/news-room/feature-stories/detail/standardization-of-vaccines-for-coronavirus-disease-covid-19.

Cette confiance est à la base des économies et sociétés numériques et axées sur les données de demain. Ainsi, il nous faudra soutenir l'élaboration non seulement de nouvelles normes, mais aussi de politiques publiques et de nouvelles lois. Bien appliquée, la normalisation souligne et promeut l'excellence. Elle vise à libérer le potentiel pour faire en sorte que les Canadiens, en plus d'avoir accès aux produits, systèmes et solutions technologiques les plus sûrs au monde, innovent en la matière – le tout en veillant à lever les obstacles qui empêchent l'accès aux marchés.

Cas d'usage : La gouvernance des données au Canada, une mise en contexte

Quand il est question de gouvernance des données et du rôle que peut jouer la normalisation dans la collecte, le partage et l'utilisation de données, il n'est pas toujours facile de conceptualiser son importance pour notre quotidien, surtout qu'il s'agit d'un actif incorporel. En vue d'aider les intervenants à comprendre l'utilité de la normalisation pour renforcer la gouvernance des données et la confiance, trois cas d'usage ont été sélectionnés pour servir d'exemples ou de témoignages pertinents. Ils touchent les données sur la santé communautaire; l'identité numérique et les systèmes bancaires ouverts; et la responsabilisation et la sécurité des consommateurs concernant les chaînes d'approvisionnement numériques en alimentation.

En période pandémique, ces cas d'usage, qui ont touché les gens et organisations personnellement, économiquement et politiquement, se sont révélés d'autant plus importants pour chaque catégorie d'intervenants au Canada.

Le premier cas d'usage sur les données sur la santé communautaire portait sur les failles en la matière dans notre système de santé. Avec la ruée récente de la population vers les soins de santé virtuels, la nécessité de disposer de mécanismes de transfert de données sûrs et efficaces s'est soudainement imposée. Statistique Canada s'est heurté à ce problème au commencement de la pandémie, lorsque la distribution d'équipement de protection individuelle aux travailleurs de la santé a été entravée par l'absence de code normalisé commun à toutes les régions de santé. Le Canada était en mesure de livrer l'équipement, mais ne connaissait pas précisément les besoins. Voilà un exemple qui illustre le rôle essentiel de la normalisation pour un travail vital.

L'augmentation récente des consultations de soins virtuels causée par la pandémie a également remis au programme la nécessité de disposer d'outils sûrs et efficaces pour permettre l'interopérabilité des données sur la santé. Les communautés ont de multiples façons d'accéder aux soins de santé. Comme la prestation des soins relève de nombreux organismes indépendants; sans protocoles appropriés, cela risque de fragiliser toute la chaîne d'approvisionnement, et la coordination des données devient de plus en plus essentielle. Lorsqu'un système n'est pas interopérable, c'est la qualité des données sur la santé qui s'en ressent. Résultat : des politiques et des décisions qui ratent leur cible, et une lenteur de l'intervention et de l'innovation dans les soins de santé. Ce cas d'usage examine comment la normalisation peut contribuer à l'adoption d'un cadre de santé communautaire canadien à l'image des valeurs et des besoins de la population.

La deuxième étude de cas porte sur les finances axées sur les clients, couramment appelées « système bancaire ouvert ». En contexte pandémique où les interactions en personne sont restreintes, la population veut maximiser le magasinage les opérations bancaires en ligne. Même en personne, mieux vaut payer avec un portefeuille numérique que sortir sa carte de crédit. Ces besoins ont mené les institutions et les gouvernements à conclure des ententes avec des tiers. Mais il manque de règlements et de normes pour encadrer ce nouveau secteur, et d'outils (comme l'identification numérique) pour qu'il soit florissant.

Ces lacunes portent préjudice aux Canadiennes et aux Canadiens – sur les plans économique et concurrentiel, et plus important encore, en matière de sécurité des données. La population a besoin de savoir que ses identifiants numériques ne seront pas vendus ou piratés. Et les petites entreprises ont besoin, elles, de se savoir appuyées par les gouvernements, avec des normes de commerce électronique qui uniformisent les règles du jeu afin que les consommateurs se sentent protégés.

La troisième étude de cas portait sur le chemin parcouru par la nourriture entre le champ et l'assiette. La chaîne d'approvisionnement de nourriture mondiale passe au numérique. Ce développement est prometteur : en accélérant la prise de décisions, il entraînerait de meilleurs résultats en matière de santé, de sécurité et d'efficacité. Mais pour que ce soit fait dans les règles de l'art et que les consommateurs puissent faire des choix alimentaires judicieux, il faut se doter de normes de gouvernance des données. En parallèle, le secteur agroalimentaire doit lui aussi garantir que sa chaîne d'approvisionnement demeure axée sur la qualité et contrôlée de bout en bout, notamment par une supervision gouvernementale stricte de la ferme à l'assiette.

Les cas d'usage ont permis au Collectif d'explorer les meilleurs moyens d'exploiter le pouvoir des données au profit des consommateurs, des gouvernements et de l'industrie. La question avait été posée : comment les technologies numériques, conjuguant confiance et transparence, pourraient-elles accélérer la prise de décisions et favoriser la santé, la sûreté et la rentabilité? La normalisation de la gouvernance des données en matière de chaîne d'approvisionnement pourrait permettre aux consommateurs de faire des choix éclairés pour leurs familles, aux gouvernements d'élaborer de meilleurs programmes de surveillance, à l'industrie d'assurer la qualité de ses produits et aux chaînes d'approvisionnement de réagir plus rapidement et ainsi d'atténuer et de minimiser les risques.

Leçons tirées des cas d'usage

À l'été 2020, le CCNGD a créé les groupes de travail sur les cas d'usage, soit de petites équipes d'experts qui se sont ensuite rencontrées à cinq ou six reprises pour vérifier l'applicabilité des enjeux globaux de la feuille de route à leurs divers secteurs. Les cas d'usage visaient non pas à concevoir des normes ou à proposer des lignes directrices, mais plutôt à pointer les lacunes pour améliorer le produit final. Chacun d'entre eux étudiait des aspects différents de la gouvernance des données qui touchaient des secteurs spécifiques.

Le groupe sur la sécurité des consommateurs a discuté de multiples systèmes d'entreposage utilisés pour la traçabilité dans l'entièreté de la chaîne de valeur de produits frais, ce qui lui a permis d'étudier la propriété et la confidentialité des données dans les secteurs suivants :

- partage de données;
- interopérabilité;
- droits des utilisateurs et identifiants;
- utilisation éthique;
- qualité et analyse des données;
- intelligence artificielle (IA) et apprentissage machine.

Le cas d'usage sur le système bancaire ouvert et l'identité numérique s'est inscrit dans une optique centrée sur l'utilisateur pour explorer des thèmes tels que :

- les exigences en matière de vérification et d'authentification de l'identité – en tenant compte de la difficulté à prouver son identité ou à avoir accès à des services en ligne pour certaines personnes;
- la propriété, l'accès et la confidentialité des données;
- les protocoles de sécurité pour le partage de données sur les clients (normes sur les API);
- les directives opérationnelles pour les risques de la mise en œuvre et de l'adoption;
- les directives relatives à l'expérience de la clientèle reflétant des valeurs d'inclusion, de transparence et de confiance.

Le groupe travaillant sur le cas d'usage des données sur la santé communautaire a adopté une vision descendante sur les principaux enjeux de gouvernance des données. Il s'est inspiré du travail mené par Statistique Canada pour la création de sa plateforme CODAS (pour collecter des données de multiples sources et les mettre à disposition de Statistique Canada et d'utilisateurs externes) et le *Cadre de renforcement des compétences et de la gouvernance en matière de données et d'information sur la santé* de l'ICIS (https://www.cihi.ca/fr/cadre-de-renforcement-des-competences-et-de-la-gouvernance-en-matiere-de-donnees-et-dinformation). Pendant les discussions sur le cycle de vie, plusieurs difficultés récurrentes ont été cernées et classées par thèmes, notamment :

- les avantages de la normalisation pour la collecte et l'encodage des données au point d'origine;
- le rôle de l'échange de données et de l'interopérabilité pour permettre l'agrégation de données;
- le rôle de lignes directrices sur l'analytique et l'étude des données qui intègrent des principes d'éthique et de transparence pour stimuler l'action.

Chaque groupe de travail a donné son point de vue sur les défis qui attendent le Canada dans ses secteurs. Tous trois ont souligné la nécessité de prendre des mesures rapidement, en s'appuyant sur ce qui avait été fait par le passé et en évitant de creuser encore davantage le fossé qui le sépare des autres pays.

Une consultation nationale a eu lieu en décembre 2020 et janvier 2021 pour discuter des effets des cas d'usage sur la population. Avec pour objectif de créer une marque et de mettre en confiance les intervenants concernant la normalisation et la gouvernance des données, elle a été l'occasion de prendre le pouls de la population relativement à l'élaboration de la feuille de route.

Plus de 160 personnes ont participé aux neuf séances (six en anglais, trois en français), notamment des représentants d'entreprises spécialisées dans la sécurité des données, d'associations et agences médicales et de soins de santé, d'institutions financières, de fournisseurs de services externes, du secteur agroalimentaire et agricole, du secteur technologique et, d'organismes gouvernementaux et réglementaires, ainsi que des conseillers stratégiques.

Les participants ont dressé le **portrait actuel** de la saisie et de l'utilisation des données numériques dans leurs champs d'intérêt respectif en matière d'identité numérique, de données sur la santé, de système bancaire ouvert et de chaîne d'approvisionnement numérique en alimentation.

Ils ont ensuite discuté de **l'avenir idéal** de la collecte de données dans ces domaines. Parmi les enjeux horizontaux communs aux trois cas d'usage, la sécurité et la confidentialité, l'interopérabilité et la normalisation, la gouvernance et la surveillance réglementaire, et l'éducation ont été évoqués.

Voici les recommandations et les considérations générales issues des séances de discussion sur les cas d'usage et de leur analyse; ces recommandations devront être intégrées au plan d'action de la feuille de route au cours de la phase II avec la mise en œuvre des solutions de normalisation.

SÉCURITÉ, CONFIDENTIALITÉ ET TRANSPARENCE

Portrait actuel : La confiance à l'endroit de la sécurité et de la confidentialité des données numériques a été un sujet récurrent. Les participants ont fait valoir que gagner et conserver la confiance des clients est la clé du succès de tout système. Les gens ont besoin de savoir quelles données personnelles seront collectées et conservées, pour combien de temps et à quelle fin; ils doivent sentir qu'ils n'ont pas à transmettre plus de renseignements que le strict nécessaire pour avoir accès à des services. Certains ont noté, par exemple, qu'il peut être difficile d'appliquer des normes de confidentialité en matière de données sur la santé et que les règles existantes ne permettent pas aux patients de donner facilement leur consentement éclairé pour le partage et l'utilisation de leurs données de santé personnelles ou d'indiquer avec précision qui héritera de leurs données en cas d'invalidité ou de décès.

Avenir idéal : Un consensus s'est dégagé autour de la nécessité de bien protéger la vie privée pour réduire les risques de partage excessif, de manipulation inadéquate ou de toute forme d'atteinte des données, de les rendre inviolables, et de garantir l'intégrité et la sécurité de leur archivage. Les gens doivent savoir comment et avec qui leurs renseignements seront partagés et pouvoir mieux contrôler l'accès à leurs données. La définition de « consentement éclairé » doit être précisée et rédigée en langage clair. Par exemple, les patients devraient pouvoir avoir accès à leurs dossiers médicaux personnels ou les partager, mais il faut un changement de paradigme fondamental : la propriété et le contrôle de données passeraient d'un modèle institutionnel à un modèle plus transparent et démocratique, centré sur le consommateur.

INTEROPÉRABILITÉ ET NORMALISATION

Portrait actuel : Un facteur clé du manque actuel d'interopérabilité des systèmes de données numériques réside dans le large éventail d'acteurs et d'autorités de réglementation de chacun des secteurs abordés. Les participants ont noté que, l'identité numérique relevant des gouvernements provinciaux, les règles actuelles varient dans chaque province et territoire, ce qui peut compliquer la transmission de données. Par exemple, la diversité et la complexité de l'industrie agroalimentaire et agricole créent un fossé entre les secteurs et les provinces, territoires et pays.

Ce fossé découle notamment d'une intégration insuffisante entre prestataires de soins de santé, de la création et de l'entreposage séparés des renseignements, d'une segmentation et d'une coopération insuffisante dans le secteur bancaire, et d'un cloisonnement des données dans l'industrie alimentaire qui limite le transfert d'information entre de nombreuses sources dans la chaîne alimentaire. Il manque de normes sur les données et la terminologie dans le système de santé du Canada, notamment pour la saisie de données. Trop peu d'efforts sont faits par le secteur agroalimentaire et agricole pour améliorer la portée et la qualité des données amassées, ce qui entraîne des lacunes persistantes dans la traçabilité des aliments et complique la tâche aux consommateurs qui souhaitent trouver de l'information sur l'origine et les méthodes de production de leurs aliments.

Avenir idéal : Il faut resserrer la normalisation des règlements sur les données pour permettre une meilleure interopérabilité aux quatre coins du pays. Ainsi, les données sur la santé pourraient circuler de façon transparente entre les systèmes, les provinces et territoires, les prestataires et les patients afin d'assurer l'équité des soins au Canada, indépendamment du lieu de résidence. Les consommateurs auraient également les renseignements nécessaires pour faire des choix alimentaires avisés et favoriser l'innovation et la mise en commun de l'information entre les secteurs et les provinces et territoires de la chaîne d'approvisionnement alimentaire. Pour y arriver, il faudra toutefois mieux numériser l'information et délaisser les systèmes papier. Par ailleurs, les participants ont fait observer que l'élargissement de la participation est un préalable à l'interopérabilité.

GOUVERNANCE ET SURVEILLANCE RÉGLEMENTAIRE

Portrait actuel : Malgré la robustesse du cadre juridique concernant la confidentialité du Canada (le pays dispose de normes de consentement parmi les plus élevées au monde), les participants ont fait valoir que les modalités sont souvent trop complexes et techniques pour que le citoyen moyen puisse comprendre et prendre une décision éclairée lorsqu'il transmet ses données financières ou sur la santé. Il y a également de grandes différences dans les lois provinciales et territoriales limitant le couplage de données sur la santé, et aucune loi ne permet un système bancaire ouvert au Canada. Les participants ont aussi mentionné que le pays est à la traîne en ce qui concerne l'élaboration de cadres législatifs et réglementaires régissant les données numériques.

Avenir idéal : L'interopérabilité n'est pas simplement une affaire de normalisation et de technologie commune; elle touche également le système législatif et réglementaire régissant les données numériques. Les participants ont souligné la nécessité d'une gouvernance et d'une surveillance efficaces, et d'établir des règles, des règlements et des normes cohérents et harmonisés d'une province et d'un territoire à l'autre. Ainsi, non seulement faciliterions-nous leur adoption et l'accès universel aux données, mais nous aiderions également à créer de nouveaux ensembles de données améliorés.

ÉDUCATION

Portrait actuel : Peu importe le sujet, les discussions ont soulevé le problème du manque de connaissances des consommateurs. Les participants aux séances sur les données sur la santé communautaire ont indiqué que la plupart des patients et des professionnels de la santé ne comprennent pas bien les règles sur les données sur la santé en vigueur au pays. Ceux des séances sur la chaîne d'approvisionnement en alimentation ont évoqué l'absence de proposition de valeur claire sur la numérisation à l'intention des acteurs des chaînes d'approvisionnement et le manque de connaissances et de compétences techniques des producteurs pour rassembler les données collectées afin de les partager dans toute la chaîne de valeurs. Les participants aux séances sur l'identité numérique et le système bancaire ouvert, quant à eux, ont invité gouvernements et industries à collaborer pour que les utilisateurs aient confiance en ce système.

Avenir idéal : Les participants aux séances sur les données sur la santé ont souligné la nécessité de former et d'informer les patients et les professionnels de la santé des règles actuelles et à venir en la matière. Ceux des séances sur l'identité numérique et le système bancaire ouvert s'entendaient sur le rôle clé que jouera l'éducation pour la concrétisation d'un modèle axé sur les consommateurs – où les gens possèdent et contrôlent leurs données – et la compréhension par ces consommateurs de l'identité numérique et de ce qu'elle implique pour eux. Les participants aux séances sur la chaîne d'approvisionnement en alimentation ont évoqué la nécessité que producteurs et fournisseurs situent mieux leur rôle potentiel dans la chaîne d'approvisionnement numérique, l'accès à la technologie nécessaire et les mesures incitatives ou mécanismes de recouvrement des coûts pour encourager l'adhésion et la participation.

Le Collectif reçoit encore des demandes concernant de prochains cas d'usage sur la gouvernance des données qui pourraient faire l'objet d'une deuxième version du présent document. Par exemple, une discussion préliminaire a eu lieu sur la surveillance des enfants et les systèmes d'apprentissage numériques et sur la nécessité de tenir des discussions verticales constantes sur la gouvernance des données; celle-ci a un effet sur divers secteurs, particulièrement depuis que la pandémie, provoquant l'utilisation accrue de systèmes d'apprentissage numériques par les enfants, a révélé des lacunes dans le domaine de la surveillance en ligne (voir le rapport de consultation préliminaire à l'annexe D). Selon ces discussions, il est clair que les prochains cas d'usage pourraient mettre de l'avant des pratiques exemplaires en matière de prestation de services de cybersécurité et de sécurité physique, ainsi que des mesures d'intervention pour accroître la sécurité numérique au Canada.

Souveraineté des données autochtones

Le CCN a confié à Firelight le mandat de concevoir, de préparer, d'administrer, d'organiser virtuellement et d'animer une première consultation autochtone dans l'ensemble du pays dans le but d'intégrer les points de vue autochtones sur la gouvernance des données au Canada à la feuille de route du Collectif. La consultation consistait en un sondage en ligne et des entrevues avec les principaux participants. Les auteurs du rapport mettent en contexte les enjeux liés à la gouvernance et à la souveraineté des données autochtones avant de résumer les résultats des consultations et de formuler des recommandations à partir des commentaires des participants. Ces derniers avaient autorisé les auteurs à utiliser leurs réponses avant de répondre au sondage ou de participer à l'entrevue.

Tout peuple a besoin de données de haute qualité sur sa population, ses communautés, son territoire, ses ressources et sa culture pour prendre des décisions éclairées, et les peuples autochtones ne font pas exception. Pourtant, ces peuples et leurs instances dirigeantes peinent toujours à obtenir leur autonomie en matière de gouvernance des données. Depuis longtemps, la collecte et la gestion des données sur les communautés autochtones sont principalement effectuées par des organismes externes; en l'absence d'un leadership autochtone, elles ne reflètent ni les priorités, ni les besoins, ni les visions du monde, ni les valeurs des communautés autochtones. Les données sont donc extraites des communautés, les indicateurs servant à mesurer la santé et le bien-être sont inadéquats, et les données sur les peuples autochtones sont mal utilisées. C'est dans ce contexte qu'émerge la notion de souveraineté des données autochtones, c'est-à-dire le droit d'une instance dirigeante autochtone de régir la collecte, la propriété, la diffusion et l'application de ses propres données sur ses communautés, ses membres, ses terres et ses ressources. Les données autochtones représentent un aspect important de la souveraineté autochtone dans son ensemble, et du mouvement vers l'autonomie gouvernementale, l'autodétermination et la décolonisation.

Dans une première étape, la consultation a pris la forme d'un sondage en ligne pour joindre le plus de monde possible dans les délais prévus. Mené en anglais et en français du 12 janvier au 2 février 2021, ce sondage visait à recueillir des commentaires sur la nature et l'importance, dans un contexte autochtone, de 10 enjeux définis par le groupe de travail 1. Au total, 36 personnes l'ont rempli. Les participants devaient classer en ordre d'importance les dix enjeux des Fondements de la gouvernance des données. Les directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique, le cadre des responsabilités, et la gouvernance de la gestion des données sont les enjeux qui ont été les plus fréquemment jugés très importants par les participants pour l'élaboration de normes sur la gouvernance des données. Aucun des enjeux n'a été jugé sans importance. Les résultats sont présentés à la section 4.1 de l'annexe C.

La firme a mené des entrevues auprès de praticiens et d'experts en gouvernance des données autochtones pour mieux comprendre les points de vue autochtones sur ces enjeux. Les participants ont été choisis en fonction de leur expertise et de leur expérience au sein d'organisations ou dans le cadre de projets et d'initiatives axés sur la gouvernance des données autochtones. Firelight s'est efforcée de recruter des experts des différents contextes propres aux Premières Nations, aux Inuits et aux Métis, dans l'ensemble du Canada. Environ la moitié des personnes invitées à une entrevue ont été en mesure d'y participer. Au total, 12 personnes ont été interrogées dans le cadre de huit entrevues. On trouvera la liste des principaux participants à la section 3.3 de l'annexe C.

Voici les grands enjeux de gouvernance des données autochtones qui se dégagent de l'analyse thématique des réponses au sondage et aux entrevues :

- Reconnaissance de l'autorité : L'autorité souveraine des gouvernements autochtones sur tous les aspects du cycle de vie des données relatives à leur population n'est pas reconnue.
- Capacité : La capacité des gouvernements et organisations autochtones de diriger la collecte, la gestion, la conservation et la communication de données, décrite en termes d'infrastructures, d'équipements, de ressources humaines, de formation, de technologie et de financement.
- Accès aux données : Souvent, les gouvernements et organisations autochtones n'ont pas accès à l'information dont ils ont besoin sur leurs populations. L'information étant hébergée par des chercheurs, des gouvernements ou d'autres organisations, les décideurs autochtones manquent des données nécessaires pour gouverner.
- Respect de la culture : Les données doivent être recueillies par des organisations autochtones, et les méthodes de collecte et de gestion de ces données doivent refléter le contexte culturel, les valeurs et les normes autochtones propres à chaque projet.

Si le rapport peut être considéré comme un premier compte-rendu des perspectives autochtones sur les enjeux de gouvernance des données et les manières possibles de s'y attaquer, il comporte un certain nombre de limites dont il faut tenir compte dans l'interprétation des résultats : peu de représentants d'organisations inuites et métisses ont participé aux consultations, et étant donné les contraintes temporelles et budgétaires, il n'a pas été possible d'aborder en détail chacun des 35 enjeux définis par les groupes de travail du Collectif. Ces limites sont expliquées plus amplement à la section 1.3 de l'annexe C.

- Les participants ont signalé l'existence de quelques normes et initiatives directement pertinentes pour l'élaboration de normes sur la gouvernance des données, qui affirment la souveraineté des peuples autochtones sur tous les aspects de la collecte, de la gestion et de l'utilisation des données : les principes de PCAP®, de la Stratégie nationale inuite sur la recherche (SNIR) et de la Stratégie de gouvernance des données des Premières Nations (SGDPN), présentés à la section 4.3 de l'annexe C.

Dans la section 5 de la même annexe, Firelight formule des recommandations basées sur les commentaires recueillis sur la consultation et la participation des groupes autochtones tout au long du processus dirigé par le Collectif.

1. Impliquer davantage les organisations et les experts en gouvernance des données inuits et métis. Étant donné leur faible participation à la consultation, il faut poursuivre les travaux pour connaître le point de vue de ces importants groupes autochtones sur les questions de gouvernance des données et sur les travaux du Collectf.
2. Impliquer davantage les groupes autochtones dans le processus du Collectif pour consacrer suffisamment de temps et de ressources à une définition claire des enjeux soulevés par les groupes autochtones et à leur intégration, le cas échéant, aux enjeux déjà définis par les groupes de travail du Collectif. Cela pourrait notamment se traduire par la participation de représentants autochtones aux groupes de travail du Collectif; pensons à un certain nombre d'enjeux définis par le groupe de travail 1 qui ont obtenu un classement élevé au sondage, comm les directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publiq le cadre des responsabilités et la gouvernance de la gestion des données, qui devront faire l'objet d'une rétroaction supplémentaire de la part des groupes autochtones.
3. Au moyen d'autres consultations, repérer les principales organisations autochtones (notamment celles qui s'occupent déjà de normalisation, comme l'Inuit Tapiriit Kanatami et le Centre de gouvernance de l'information des Premières Nations) en vue de les impliquer dans les prochaines étapes des travaux du Collectif, y compris la normalisation elle-même.

Enjeux et recommandations

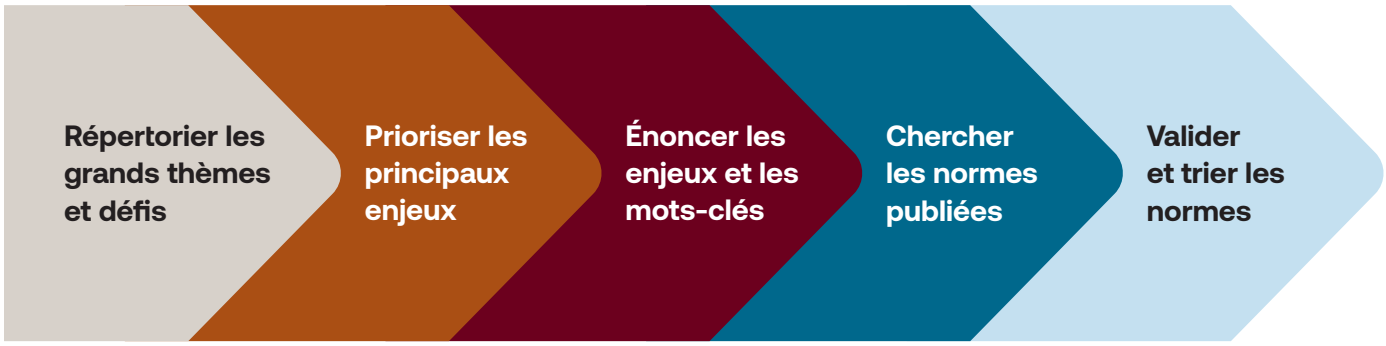
Cerner les principaux enjeux

En janvier 2020, les secteurs prioritaires de la feuille de route ont été limités à 35 enjeux, car étant donné la complexité de la gouvernance des données, il aurait été impossible de traiter de l'ensemble. L'évaluation de la pertinence des normes pour la gouvernance des données s'est révélée une tâche colossale vu l'ampleur du sujet et des défis posés par les nouvelles technologies dans l'ensemble de la chaîne d'approvisionnement et du cycle de vie de la gouvernance des données.

Sur une période d'un an, le groupe de travail s'est réuni en ligne pour décrire et délimiter les enjeux choisis, répertorier les normes actuelles, mener une analyse des lacunes et rédiger la feuille de route. Pour ce faire, le Collectif a employé une méthode de recherche participative afin de permettre à tous les membres des groupes de travail d'apporter leur expertise et leur perspective au processus de production des connaissances, c'est-à-dire à l'élaboration de la feuille de route[14]. Plus précisément, chaque groupe de travail a suivi les étapes ci-dessous pour dessiner le paysage normatif actuel dans chaque enjeu.

14 Bergold, J. et S. Thomas (2012). « Participatory research methods: A methodological approach in motion ». Historical Social Research/Historische Sozialforschung, vol. 37, no 4, p. 191-222.

Diagramme 1 : Portrait du paysage normatif



En tout, près de 12 000 normes ont été répertoriées pour les 35 enjeux (on trouvera la méthode de sélection à l'annexe G[15]). L'étape suivante consistait à valider et à trier les normes et à transmettre le résultat aux organismes d'élaboration de normes concernés pour avoir leur avis et leur validation. Nous avons également demandé à des organismes d'élaboration de normes nationaux et internationaux de fournir la liste des normes en cours d'élaboration susceptibles d'apporter des solutions aux 35 enjeux répertoriés.

À partir de cette liste, les groupes de travail ont analysé les lacunes des normes, spécifications et programmes d'évaluation de la conformité actuels et nécessaires pour chaque enjeu. Était considérée comme une « lacune » l'absence de norme ou de spécification ou d'autre document publié couvrant l'enjeu en question. Chacune était évaluée et classée par ordre de priorité : élevée (à combler en moins de deux ans), moyenne (à combler en deux à cinq ans) ou faible (à combler en plus de cinq ans). De ce processus a découlé un projet de feuille de route (au diagramme 3 à la fin de la section Recommandations), confirmé par les coprésidents des groupes de travail, qui comporte des suggestions d'activités de mise en œuvre.

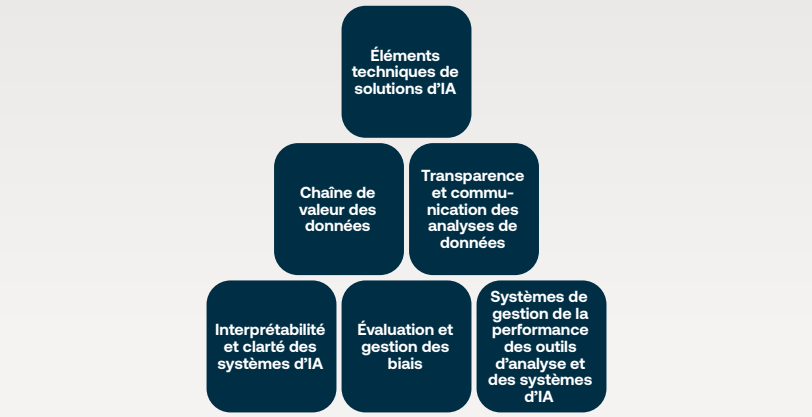
À la feuille de route s'ajoute le *Paysage normatif du CCNGD*, un tableau des normes liées (directement ou indirectement) aux enjeux décrits dans la feuille de route, que l'on trouvera à l'annexe I.

Nous l'avons dit : la feuille de route s'attaque aux enjeux en adoptant un modèle de cycle de vie des données, complexe et dynamique, en évolution et en adaptation constantes, qui implique plusieurs parties. Nous avons reconnu dès le départ que l'analyse de la gouvernance des données peut se faire sous divers points de vue et aspects.

C'est dans cette optique que les activités d'élaboration de la feuille de route ont été regroupées sous quatre grands thèmes, ensuite attribués à quatre groupes de travail : 1) Fondements de la gouvernance des données, 2) Collecte, organisation et classement, 3) Accès, diffusion et conservation, et 4) Analyse, solutions et commercialisation. Ces domaines ont été divisés en sujets d'intérêt en lien avec les normes et les programmes d'évaluation de la conformité sur la gouvernance des données comme l'illustre l'image ci-dessous.

15 Au départ, la recherche des quelque 500 mots-clés a généré environ 25 000 normes, dont plus de la moitié étaient des doublons à supprimer.

Diagramme 2 : Thèmes et principaux enjeux de gouvernance des données



Analyses, solutions et conservation
Concepts propres à la catégorie du cycle de vie

Accès, diffusion et conservation
Concepts propres à la catégorie du cycle de vie

Collecte, organisation et classement
Concepts propres à la catégorie du cycle de vie

Fondements de la gouvernance des données
Normes fondamentales : concepts généraux, exigences communes, généralement applicables

Recommandations

Voici un résumé des recommandations concernant les 35 enjeux à l'étude; il comprend des témoignages qui les mettent en contexte et montrent leur effet sur les utilisateurs et les organisations. Elles visent à orienter les discussions à venir sur la correction des lacunes répertoriées et à montrer comment la normalisation peut renforcer la confiance et faire de nous des premiers de classe mondiaux dans l'élaboration de produits, systèmes et solutions sécuritaires. Le résumé n'est pas final et doit être lu en parallèle avec l'annexe A, qui décrit plus avant les discussions sur les principaux enjeux. À l'étape de l'élaboration des plans d'action visant à mettre en œuvre les recommandations, il faudra commencer par analyser chaque enjeu à la lumière des rapports sur les cas d'usage et la consultation autochtone (annexes D et C) ainsi que sur le paysage normatif (annexe I). On trouvera à l'annexe B une version abrégée du paysage comportant une liste de normes et d'autres types de documents normatifs pertinents.

Groupe de travail 1 : Fondements de la gouvernance des données

Enjeu 1 – Cadre de responsabilité

Portée : La structure de responsabilité et de contrôle pour toutes les données créées ou recueillies, y compris les rôles et responsabilités en matière de traitement des données, les conséquences d'un transfert de propriété, la notion de consentement, la conformité et la responsabilité dans la réglementation.

Témoignage d'utilisateur : Comme parent canadien d'un enfant en milieu d'apprentissage numérique, j'ai besoin de transparence sur le consentement des plateformes d'apprentissage en ligne que mon enfant utilise et sur la collecte de ses données et leur utilisation à d'autres fins. Comment puis-je savoir que ces plateformes sont conformes aux réglementations en matière de confidentialité?

Recommandation : Élaborer des pratiques exemplaires nationales ou des solutions de normalisation pour les cadres de responsabilité liés à la confidentialité et à la sécurité des renseignements personnels.

Enjeu 2 – Attestation encadrant les rôles professionnels

Portée : L'évaluation du rôle des professionnels qui traitent les données et l'information, soit les exigences en matière de compétences professionnelles en fonction d'un cadre clair qui formera la colonne vertébrale de la gouvernance des données.

Témoignage d'utilisateur : En tant que citoyen, je veux savoir que les entreprises auxquelles je confie mes données s'engagent à faire respecter les normes de l'industrie.

Recommandation : Élaborer des critères ou normes pour évaluer les compétences de bases des professionnels de la gouvernance des données.

Enjeu 3 – Habileté numérique

Portée : L'amélioration de la compréhension des données, des technologies et des interfaces destinées à la population canadienne.

Témoignage d'utilisateur : En tant que citoyen, je veux comprendre les paramètres de confidentialité et la protection par mot de passe, et utiliser des services en ligne dans un environnement sécuritaire.

Recommandation : Élaborer des normes accessibles à différentes couches de la société : jeunes, personnes âgées, groupes vulnérables ou communautés qui n'ont ni l'anglais ni le français comme langue maternelle, entre autres.

Enjeu 4 – Cybersécurité et protection des données

Portée : La cybersécurité et la transparence, des éléments transversaux d'un cadre de gouvernance des données; notamment les infrastructures numériques, de réseau et de connectivité, sans toutefois couvrir la sécurité des TI (l'aspect physique des infrastructures).

Témoignage d'utilisateur : Comme propriétaire d'une petite entreprise, comment puis-je mieux gérer la cybersécurité et faire en sorte que mes clients aient confiance en mes services?

Recommandation : Miser davantage sur les solutions de normalisation intersectorielles (et non les normes sectorielles encadrant la résilience et la sécurité de l'information) en matière de cybersécurité.

Enjeu 5 – Gouvernance de la gestion des données

Portée : La planification, la supervision, la surveillance et l'application de la gestion des données à l'échelle organisationnelle, qui visent à expliciter la manière de gérer les données tout au long de leur cycle de vie.

Témoignage d'utilisateur : En tant qu'expert responsable du système de gestion des données de mon organisation, quels outils ou directives me permettraient d'optimiser la productivité de mon entreprise, de gérer les risques pour sa sécurité et de prendre les bonnes décisions?

Recommandation : Normaliser la gouvernance organisationnelle de la gestion des données adaptée à des organisations de diverses tailles et de divers types.

Enjeu 6 – Protection des renseignements personnels (enjeu regroupé avec celui des droits sur les données)

Portée : Le processus qui consiste à déterminer à qui reviennent les droits sur les données, si ces droits peuvent être cédés et qui peut diffuser les données. Le contrôle de l'information est un sujet de plus en plus pertinent, surtout maintenant que de nouvelles données peuvent être employées et générées par l'IA et l'Internet des objets. Les renseignements générés par ces nouvelles technologies devraient donc aussi être transparents, conformes et équitables que les autres, et leur diffusion consentie par le détenteur des droits. La Charte canadienne des droits et libertés devrait aussi servir de guide.

Témoignage d'utilisateur : En tant que citoyen, quels droits ai-je sur mes données personnelles? Comment les organisations qui les détiennent se conforment-elles aux règlements et aux lois? Comment est-ce que je consens à l'utilisation de mes données personnelles?

Recommandation : Harmoniser les lois sur la vie privée et la sécurité au Canada, notamment en ce qui a trait au consentement, en utilisant des solutions de normalisation au besoin.

Enjeu 7 – Directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique

Portée : L'établissement de la fiabilité et de l'éthique dans l'utilisation des données par rapport aux attentes canadiennes en matière de renseignements personnels énoncées dans la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*, ce qui consiste à clarifier les aspects éthiques de la propriété des données, notamment leur utilisation éthique et sociale en fonction de leur valeur publique.

Témoignage d'utilisateur : En tant que citoyen, comment puis-je savoir qu'une organisation respecte la *Loi sur la protection des renseignements personnels et les documents électroniques* ou la *Loi sur la protection des renseignements personnels*? Quelles sont mes garanties?

Recommandation : Normaliser les responsabilités de l'ensemble des acteurs impliqués dans le cycle de vie des données.

Enjeu 8 – Données ouvertes et procédures d'harmonisation et d'interopérabilité des données

Portée : L'harmonisation des pratiques relatives aux données visant à couvrir les rapports entre la technologie, les procédures et les systèmes. L'enjeu couvre également l'utilité des pratiques stratégiques, légales et commerciales pour faciliter l'interaction entre entreprises et industries. Plutôt que de pratiques techniques, on parle donc ici d'interopérabilité au sens général, particulièrement de la possibilité de transférer des données d'une plateforme à une autre avec le plus de précision et le moins d'interventions possible, tout en assurant la sécurité et la confidentialité des renseignements.

Témoignage d'utilisateur : Employé d'un organisme de soins de santé, j'ai besoin d'une intégration rapide de données provenant de diverses sources. J'ai besoin de pratiques et de politiques harmonisées pour évaluer les besoins d'interopérabilité de l'écosystème de santé dans lequel je travaille, tout en protégeant la vie privée de mes patients.

Recommandation : Promouvoir l'harmonisation et l'interopérabilité des nouvelles technologies et pratiques, appuyées par des solutions de normalisation s'il y a lieu.

Enjeu 9 – Rôles des acteurs et des opérations en matière de traitement des données

Portée : Exploration du rôle des acteurs qui participent au cycle de la vie de la chaîne d'approvisionnement et mise en lumière des responsabilités des professionnels. De la collecte à l'utilisation des données interviennent un grand nombre de processus de traitement. Peu importe la quantité de données, leur cycle de vie implique beaucoup de personnes et de systèmes informatiques. Qu'il s'agisse de protection contre les accès non autorisés ou de sauvegardes quotidiennes, par exemple, ces divers acteurs sont responsables de protéger les données en créant un système sécurisé qui réduit les risques d'erreurs. L'enjeu englobe la terminologie normalisée sur le rôle de chaque système informatique (et de chaque utilisateur) et de ce que cela implique pour le fournisseur, le consommateur, le courtier, l'utilisateur, le référentiel, etc.

Témoignage d'utilisateur : En tant que citoyen, comment puis-je savoir qu'une organisation emploie des professionnels qualifiés pour gérer mes données (ou les siennes)? Quelle est l'imputabilité de ces employés?

Recommandation : Poser les fondements de normes intersectorielles pour faciliter la supervision des professionnels des données dans l'ensemble des secteurs.

Enjeu 10 – Réutilisation des données

Portée : Réutilisation de données à d'autres fins que celles qui étaient prévues. Elle comprend l'utilisation qui vise un objectif différent de celui qui a été accepté par le détenteur des droits sur les données et pour lequel il n'a pas donné de consentement explicite. L'enjeu explore la possibilité de détruire des données et de retirer son consentement, ainsi que l'expiration du consentement.

Témoignage d'utilisateur : En tant que citoyen, comment puis-je savoir si mes données sont vendues à d'autres utilisateurs et comment puis-je y consentir?

Recommandation : Élaborer des pratiques exemplaires pour permettre une gestion dynamique du consentement et l'utilisation de données dépersonnalisées, balisées par une normalisation et un cadre de gouvernance stricts, comme avantage compétitif.

Groupe de travail 2 : Collecte, organisation et classement

Enjeu 11 – Collecte des données

Portée : La collecte et la quantification de l'information sur des variables d'intérêt. Déterminer la nécessité, en ce qui concerne l'acquisition de données, de trouver un équilibre entre utilité et moyens employés pour les obtenir.

Témoignage d'utilisateur : En tant que citoyen dont les données sont hébergées sur de multiples plateformes de stockage, la confiance est pour moi essentielle. Il est crucial de créer d'un système ou un outil permettant d'évaluer si mes données sont recueillies dans le respect de principes d'acquisition éthique.

Recommandation : Normaliser cette pratique et couvrir les trois catégories de sources de données : analogiques, numériques et dynamiques.

Enjeu 12 – Gestion des systèmes de données

Portée : La gestion des systèmes de données visant à garantir l'interopérabilité et la sécurité qui passent par la conception, le chiffrage et les contrôles d'accès.

Témoignage d'utilisateur : En tant que citoyen, je crois qu'il faut que les systèmes de données soient dotés de contrôles d'accès pour intégrer divers types de données et les transformer afin qu'elles puissent être utilisées en toute sécurité.

Recommandation : Normaliser la communication entre les mécanismes et les appareils dans les systèmes. Il faut clarifier si la gestion des systèmes dépend du type de données hébergées et s'il faut différents groupes de normes pour l'encadrer. Par exemple, on pourrait considérer cette gestion comme une application servant à intégrer, manipuler et supprimer des données. Se pose aussi la question de savoir si les normes sont appliquées à toutes les opérations ou étapes du cycle de vie des données.

Enjeu 13 – Visibilité des données

Portée : La connaissance des jeux et des sources de données existants, de leur localisation et de leur mode d'utilisation; cela exclut la notion que la simple possibilité de trouver des données en garantisse l'accès.

Témoignage d'utilisateur : En tant que citoyen dont les données sont hébergées sur plusieurs plateformes, j'ai besoin de pouvoir trouver facilement l'information stockée à mon sujet.

Recommandation : Normaliser la configuration des systèmes d'extraction des données et de la taxonomie des données existantes. Il est essentiel de savoir comment les données sont interprétées, numérisées, recueillies et formatées, car cela a un lien avec les méthodes d'interprétation et d'analyse pour le couplage.

Enjeu 14 – Couplage des informations

Portée : Le couplage des informations de deux ou de plusieurs sources pour enrichir un jeu de données. Il recoupe des enjeux de consentement et de sécurité, puisque les données ne viennent pas du même endroit.

Témoignage d'utilisateur : En tant que citoyen, je dois pouvoir avoir confiance en la façon dont mes données seront utilisées et couplées. Il faut une meilleure surveillance des pratiques susceptibles de créer de l'information rattachable à un individu par le couplage de fichiers de données indépendants.

Recommandation : Normaliser le couplage de données en prenant en compte et en atténuant les répercussions sur la vie privée. Le couplage pose un dilemme éthique qui va au-delà de la visée première de la collecte de données.

Enjeu 15 – Marquage manuel des données

Portée : Ajout manuel de données par intégration de codes particuliers plutôt que d'algorithmes d'IA pour corriger les erreurs possibles d'un système automatisé.

Témoignage d'utilisateur : En tant que citoyen, je suis préoccupé par la façon dont un système génère des données. Par exemple, si un système de reconnaissance faciale véhicule un préjugé, il est probable qu'il oriente les résultats.

Recommandation : Normaliser le marquage manuel des données pour créer une combinaison de méthodes visant à réduire les erreurs générées par les systèmes automatisés. L'absence d'approche commune entraîne des préjugés.

Enjeu 16 – Gestion des métadonnées

Portée : La gestion des données qui donnent de l'information sur d'autres données. Cette pratique englobe l'entièreté du processus de collecte, de gestion, d'accès et de compréhension des capacités des données. La gestion des métadonnées, les « données sur les données », peut établir leur fiabilité.

Témoignage d'utilisateur : En tant que citoyen, si je comprends la terminologie qui décrit les données sur les données, j'arrive à mieux évaluer la fiabilité des données stockées. Par exemple, les résultats d'essais cliniques pour un vaccin me donnent une idée de son efficacité.

Recommandation : Normaliser la terminologie associée à la gestion des métadonnées.

Enjeu 17 – Politiques sur les données : gestion des risques et stratégies dans les organisations

Portée : L'assurance de la conformité par l'adoption d'un cadre de gouvernance des données.

Témoignage d'utilisateur : En tant que citoyen, je ferais plus confiance aux systèmes de gestion de données si l'ensemble des organisations se dotaient de politiques et de pratiques de gestion des risques uniformes pour créer un cadre de gouvernance des données. Par exemple, la politique de l'entreprise de télécommunication A exige la conservation des renseignements personnels pendant trois ans, tandis que celle de l'entreprise B parle de sept ans.

Recommandation : Normaliser la création de cadres stratégiques et de cadres de gestion des risques dans les organisations.

Enjeu 18 – Qualité et aptitude à l'emploi des données

Portée : L'évaluation de la qualité des données et l'ensemble des activités qui s'y rattachent.

Témoignage d'utilisateur : En tant que citoyen, je veux avoir confiance en la qualité des données hébergées par des magasins de données.

Recommandation : Normaliser les cadres en place pour comprendre, décrire, surveiller, vérifier et prouver la qualité des données, ainsi que pour en faire état.

Groupe de travail 3 : Accès, diffusion et conservation

Enjeu 19 – Gestion du consentement (consentement, accès et retrait)

Portée : La gestion de l'entièreté du cycle de vie du consentement explicite d'utilisation de données (version papier ou numérique) entre une personne (ou propriétaire de données) et un responsable (ou fournisseur, ou consommateur).

Témoignage d'utilisateur : En tant que patient qui consent à ce que mon fournisseur de soins collecte des données à mon sujet à des fins diagnostiques, je dois avoir la possibilité de retirer mon consentement afin d'éviter que mes données soient utilisées une fois mon problème de santé résolu.

Recommandation : Normaliser le consentement et sa portée (élément de données précis ou large éventail de sujets connexe, données acquises dans le passé ou dont l'acquisition est prévue dans le futur); la gestion des formes numériques du consentement sur tout leur cycle de vie; leur nécessité et leur application pour chaque transfert et échange de données; et l'effet de leur retrait sur les données déjà partagées.

Enjeu 20 – Accès aux données

Portée : L'établissement d'une connexion entre un fournisseur de données et un ou plusieurs consommateurs dans un but d'extraction, soit la sélection du jeu de données, l'élaboration et la négociation d'un contrat d'utilisation bilatéral ou multilatéral, ainsi que l'application des politiques et de restrictions contenues dans ce contrat.

Témoignage d'utilisateur : En tant que fournisseur, je dois être en mesure d'empêcher les consommateurs de le transmettre un jeu de données à un tiers et ainsi garder entièrement le contrôle des données auxquelles je donne accès.

Recommandation : Normaliser l'élaboration et la négociation des contrats d'accès entre fournisseurs et consommateurs de données avec des politiques d'utilisation compréhensibles à la fois pour des machines et des humains, et, par le fait même, interopérables, et l'application de ces contrats avec leurs restrictions et leurs obligations pendant l'extraction et après, lors de la transmission des données à un consommateur.

Enjeu 21 – Conservation des données

Portée : La gestion de l'information relative à un élément de donnée tout au long de son cycle de vie – acquisition, circulation entre les acteurs, modification et nouvelles données qui en émergent (ou qui y sont liées).

Témoignage d'utilisateur : En tant que propriétaire de données qui héberge ses données chez un fournisseur, je dois être en mesure de définir les règles qui régissent leur conservation pour m'assurer de ne jamais perdre d'information importante.

Recommandation : Normaliser l'expression des règlements et des politiques de conservation qui régiront la gestion du cycle de vie des données par les intendants, y compris l'archivage, la transformation, la compression et la mise hors service des données de façon sécuritaire, transparente, portable et conforme. Il faudrait également normaliser certains aspects qui touchent à d'anciens formats et outils de données qui, sans traitement approprié, pourraient rendre les données conservées inutilisables.

Enjeu 22 – Gestion de l'identité : validation et authentification (individus, identités et appareils)

Portée : La gestion et l'utilisation d'identifiants numériques dans le but d'authentifier l'identité d'un acteur des données (individu, organisation ou appareil), permettant ensuite la conclusion de contrats d'utilisation et le traitement de données en toute sécurité, par voie numérique.

Témoignage d'utilisateur : En tant que citoyen, je dois pouvoir choisir mon fournisseur d'identité pour signer numériquement des documents de consentement.

Recommandation : Normaliser l'attribution, l'utilisation et la gestion des identifiants numériques afin que leurs acteurs (individus, organisations et appareils) puissent participer de manière sécuritaire au traitement des données, notamment la fédération et l'authentification dans divers réseaux d'identité pour le respect des politiques d'accès aux données, mais aussi de restrictions dans l'échange de données et le traçage de participants à d'anciennes transactions.

Enjeu 23 – Partage, échange et intégration de données

Portée : Les principes directeurs du partage, de l'échange et de l'intégration de données et leur application à des ententes normalisées. Comme les données sont des ressources non rivales (c. à d. qu'elles peuvent utilisées simultanément après copie), il faut des mécanismes aux propriétaires de données pour exercer leur souveraineté sur leurs données après leur transmission ou leur intégration à un bien qu'ils ne contrôlent pas directement.

Témoignage d'utilisateur : En tant que propriétaire de données, j'ai besoin d'une façon de définir les modalités de transmission, de communication et d'intégration de mes données à d'autres produits et services afin de pouvoir contribuer aux causes qui me tiennent à cœur.

Recommandation : Normaliser les ententes et les cadres de partage de données en se concentrant sur les aspects contractuels plutôt que sur les aspects techniques, y compris tous les scénarios de transmission et d'échange de données (bilatéral, multilatéral et décentralisé) et leur intégration, c'est-à-dire lorsqu'elles deviennent partie intégrante d'un autre bien (produit, service ou regroupement).

Enjeu 24 – Fiabilité des intermédiaires du traitement des données

Portée : Le rôle des intermédiaires (courtier en information, fiducies de données, syndicats et collectifs de l'information) qui assurent l'intendance fiduciaire indépendante, de manière temporaire ou permanente, des données, et la séparation du stockage et de la gestion des applications de production ou de gestion de données qui en découle.

Témoignage d'utilisateur : En tant que citoyen, je dois pouvoir conserver tous mes dossiers financiers à un seul endroit. Il me faut un organisme indépendant auquel mes services financiers enverraient mes données et auquel je permettrais à d'autres services financiers de demander ces données.

Recommandation : Élaborer des normes applicables aux intermédiaires du traitement des données pour le stockage ou le courtage indépendants, qui leur permettraient de prouver leur fiabilité au sein de l'écosystème. Elles préciseraient les conditions dans lesquelles les intermédiaires pourraient prendre des décisions sur les données au nom de leur propriétaire, de même que les modalités d'application des contrats d'utilisation mis en place par les propriétaires qui leur permettraient de transférer, de manière temporaire ou permanente, des données dont ils sont responsables.

Enjeu 25 – Autorisation à la collecte et au partage de données

Portée : Les politiques qui régissent la collecte de données personnelles et industrielles ou commerciales ainsi que les permissions, restrictions et obligations des acteurs qui les collectent en ce qui a trait à leur partage, y compris les mécanismes qui encadrent ces politiques et assurent la transparence de l'encadrement tout en protégeant les renseignements confidentiels.

Témoignage d'utilisateur : En tant que citoyen, je veux une transparence complète : savoir qui est autorisé à collecter des données à mon sujet et à quelles fins, afin d'avoir la garantie que ma vie privée est respectée.

Recommandation : Normaliser les politiques de collecte de données, les modalités d'autorisation de collecte et de délivrance de cette autorisation, les conditions permettant leur traitement et leur partage sous forme d'information regroupée, et les conditions permettant l'extraction de données particulières d'un tel jeu de données regroupées.

Enjeu 26 – Chiffrage

Portée : Les politiques et les normes qui régissent l'utilisation d'outils techniques pour encoder les renseignements confidentiels à tous les stades de leur cycle de vie – les données inactives, les données en transit et les données utilisées – couvrant notamment le type (y compris le chiffrage homomorphique), la force, l'application, l'utilisation du chiffrage pour garantir l'intégrité des données et les acteurs qui peuvent traiter les données chiffrées (et déchiffrées) et les circonstances de ce traitement.

Témoignage d'utilisateur : En tant que propriétaire de données, je veux avoir la certitude que mes données seront chiffrées par tous les acteurs du traitement des données, pour toutes les opérations, et qu'elles seront déchiffrées seulement par ceux à qui je transmets une clé privée ou à qui je donne mon consentement explicite.

Recommandation : Normaliser l'utilisation du chiffrage et ses critères d'acceptation pour la conformité aux règles de confidentialité tout en utilisant des données qui tiennent compte du potentiel des nouvelles technologies (comme les ordinateurs quantiques).

Enjeu 27 – Gestion des ontologies

Portée : La gestion des ontologies individuelles (vocabulaire de concepts, hiérarchies et relations), l'organisation d'ontologies multiples (regroupement, fusion et liens) et leur utilisation pour l'encodage.

Témoignage d'utilisateur : En tant que consommateur de données, je veux pouvoir traduire le jeu de données obtenu d'un fournisseur en l'ontologie de mon choix afin de pouvoir interpréter les données en utilisant ma propre terminologie.

Recommandation : Normaliser la gestion des ontologies (vocabulaires de concepts, hiérarchies, relations, etc.) et leur cycle de vie (de la définition à l'élimination d'un concept), ainsi que leur application à la description des données et de leur sens, y compris les pratiques d'encodage complexes (postcoordination et précoordination), et aussi la façon dont les consommateurs de données auront accès à l'ontologie décrivant le jeu de données qu'ils extraient.

Enjeu 28 – Transparence, parcours et traçabilité des données

Portée : La gestion de l'information concernant la manipulation et le traitement d'un élément de de donnée dans l'entièreté de son cycle de vie – acquisition, circulation entre les acteurs, modification et les nouvelles données qui en émergent (ou y sont liées).

Témoignage d'utilisateur : En tant qu'utilisateur des infrastructures publiques de la ville, j'ai besoin de savoir quelles données de mobilité sont collectées à mon sujet, qui les utilise et à quelles fins afin de connaître ma contribution à la création d'une ville intelligente.

Recommandation : Normaliser l'information amassée sur un élément de données acquis, échangé, modifié et utilisé comme autre source de production ou d'analyse de données, l'accès et les conditions d'accès à cette métainformation, ainsi que les modalités de sa protection, de sa conservation et de son élimination, indépendamment de l'élément de donnée qu'elle décrit.

Enjeu 29 – Portabilité et mobilité des données

Portée : Le droit à la portabilité des données donne aux sujets concernés accès aux renseignements personnels qu'ils ont fournis à un responsable dans un format structuré, couramment utilisé et lisible par machine, tout en permettant la transmission sécurisée de ces données entre responsables.

Témoignage d'utilisateur : En tant que citoyen utilisateur d'un réseau social, je dois pouvoir demander l'exportation en format numérique de toutes mes données sur ce réseau pour pouvoir les stocker dans un référentiel de mon choix.

Recommandation : Normaliser la conservation de l'échange d'information entre systèmes afin que les données puissent être exportées en format numérique par des responsables avec leur structure détaillée, les métadonnées et les liens vers d'autres données, ainsi que les circonstances où les données peuvent être supprimées par un responsable et les implications de la suppression sur les autres données liées (ex. : le droit à l'oubli).

Groupe de travail 4 : Analyses, solutions et commercialisation

Enjeu 30 – Éléments techniques des solutions d'IA

Portée : Les éléments techniques et le cycle de vie des solutions d'IA concernant les systèmes, technologies, logiciels et plateformes et leur développement, leur analyse, leur vérification et leur validation, ce qui englobe la terminologie employée (y compris l'IA comme telle), les sous-catégories d'IA, la description du cycle de vie et chacune des composantes.

Témoignage d'utilisateur : En tant que citoyen ou en tant que praticien de l'IA, je veux comprendre la terminologie utilisée pour décrire les solutions qui utilisent mes données et avoir la certitude qu'elles fonctionnent comme prévu.

Recommandation : Normaliser la terminologie et les éléments du cycle de vie pour jeter les bases de l'interopérabilité des solutions d'IA et des spécifications de vérification et de validation.

Enjeu 31 – Chaînes de valeur des données

Portée : La valeur financière créée à diverses étapes de la chaîne d'approvisionnement. La détermination de la valeur financière et l'évaluation des données, et leur rôle dans la propriété intellectuelle.

Témoignage d'utilisateur : En tant que citoyen, je veux m'assurer d'avoir un juste retour sur les données que je partage. En tant que propriétaire d'une entreprise de données, je souhaite monétiser les données pour en tirer un revenu.

Recommandation : Normaliser le système qui attribue une valeur aux données et ses implications pour les échanges et les opérations.

Enjeu 32 – Transparence et communication des analyses de données

Portée : La communication des analyses de données, de même que des risques pour les propriétaires de données du point de vue de la chaîne d'approvisionnement.

Témoignage d'utilisateur : En tant que citoyen propriétaire de données, je veux connaître l'utilisation qui en est faite et les risques associés à leur partage.

Recommandation : Normaliser la méthode et la terminologie utilisées pour informer les propriétaires de ce qui est fait de leurs données et des risques potentiels de leur partage.

Enjeu 33 – Interprétabilité et clarté des systèmes d'IA (d'abord appelé « Interprétabilité des algorithmes)

Portée : L'explication des résultats, des capacités et des fonctions d'un algorithme. Dans ce contexte, l'explicabilité signifie que les résultats peuvent être compris par des humains.

Témoignage d'utilisateur : En tant que citoyen, j'entre en contact avec des solutions d'IA par les produits et services que j'utilise. Je veux connaître leurs capacités, les résultats ou les décisions qu'elles peuvent produire et les *raisons* de ces décisions.

Recommandation : Normaliser l'explication des capacités et des résultats des systèmes d'IA en termes compréhensibles par les humains.

Enjeu 34 – Évaluation et gestion des biais

Portée : Le repérage des biais et, s'il y a lieu, leur gestion.

Témoignage d'utilisateur : En tant que citoyen, je veux m'assurer de ne pas être victime de biais ou de discrimination en raison d'une décision prise par une solution d'IA ou avec son aide, surtout lorsque cela a des répercussions sur mes finances, mes assurances ou ma santé.

Recommandation : Normaliser les types de protocoles, de processus et d'évaluations utilisés pour repérer les biais, ainsi que la gestion des biais, s'il y a lieu.

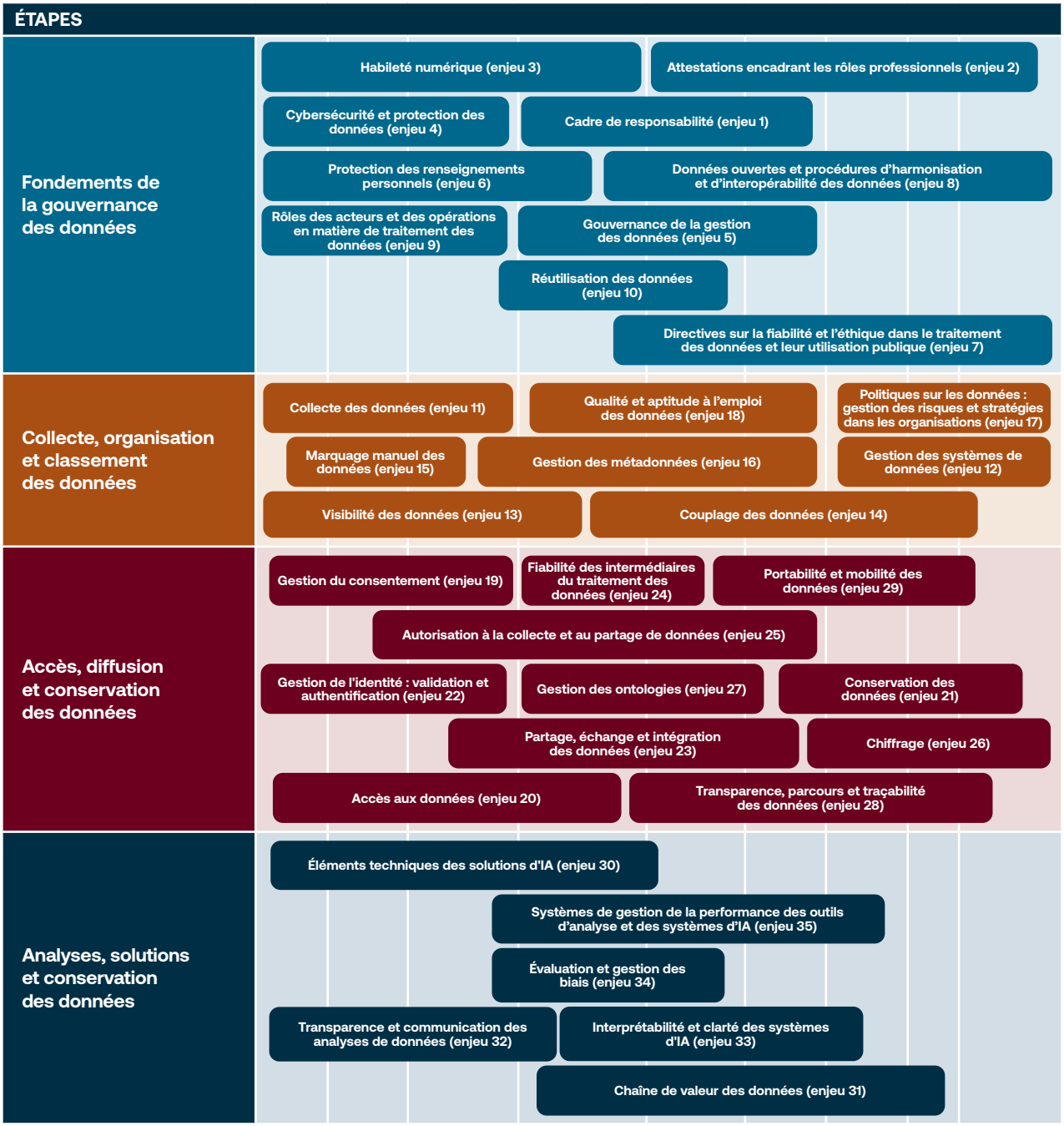
Enjeu 35 – Systèmes de gestion de la performance des outils d'analyse et des systèmes d'IA

Portée : La mise en place d'une gouvernance interne, de l'analyse du niveau de risque à la conception et au déploiement de modèles, d'algorithmes et de systèmes.

Témoignage d'utilisateur : En tant que citoyen, je veux avoir l'assurance que les organisations qui développent ou utilisent des solutions d'IA disposent des bons processus pour garantir la qualité des systèmes qu'ils créent et qu'ils utilisent, et des bons processus pour gérer les désagréments ou les imprévus.

Recommandation : Normaliser les approches de gouvernance des organisations qui utilisent ou créent des systèmes d'IA, en encourageant une participation diversifiée dans l'élaboration de normes fondées sur l'évaluation de la conformité comme la norme ISO/IEC 42001 sur les systèmes de management de l'intelligence artificielle.

Diagramme 3 : Échéancier proposé pour la mise en œuvre de la feuille de route



Étapes suivantes

Cette feuille de route est une première étape dans l'élaboration d'un vocabulaire et d'un langage commun à l'ensemble des acteurs qui, stimulés par les possibilités techniques, les politiques et la pression de la concurrence, cherchent à faire évoluer leurs stratégies et leurs cadres de données. Elle propose la normalisation comme voie vers la compréhension et la résolution des enjeux stratégiques et opérationnels de gouvernance des données auxquels le Canada, tout comme d'autres pays, est aujourd'hui confronté.

L'agilité du système de normalisation en constante redéfinition nous appelle à appréhender de nouvelles notions : la dépersonnalisation et l'anonymisation mises de l'avant par de nouvelles lois sur la vie privée (projet de loi nº 64 et le projet de loi C-11), ou les règles sur l'utilisation et la gestion des systèmes d'IA dans les nouvelles réglementations mondiales. Il faudra notamment établir les limites de la normalisation comme outil optimal pour concrétiser la vision, limites au-delà desquelles il faudra des politiques ou d'autres facteurs. Si la cartographie de la normalisation est utile sur le coup, l'évolution rapide de la technologie fait en sorte qu'une fois publié, le paysage normatif est vite dépassé. Le Canada et les écosystèmes concernés tireront avantage du maintien du Collectif, qui révisera régulièrement ce travail, tiendra la feuille de route à jour et surveillera la mise en œuvre de ses recommandations dans l'ensemble du pays.

Comme le montre le diagramme 3, il y a douze enjeux pour lesquels nous devons nous mettre au travail dès maintenant, à commencer par l'habileté numérique, la cybersécurité et les renseignements personnels. L'adoption, l'adaptation et l'élaboration de normes et d'activités d'évaluation de la conformité pour combler les lacunes actuelles et mettre en œuvre les 35 recommandations nécessiteront soutien et leadership. Il faudra également une analyse et des plans d'actions détaillées pour chacun des enjeux et des résultats des groupes de travail sur les cas d'usage, la consultation autochtone et le paysage normatif afin que les activités qui sont déjà en cours d'élaboration tiennent compte des normes, pratiques exemplaires et autres documents normatifs avec l'évolution des initiatives.

De même, il faut intégrer les recommandations de la consultation autochtone directement au plan de mise en œuvre, notamment par : 1) une mobilisation accrue des organisations, détenteurs de droits et intervenants métis et inuits, mal représentés dans la première version de cette feuille de route; 2) l'implication de groupes autochtones pour rattacher directement les conclusions du mandat de Firelight aux enjeux soulevés par les groupes de travail sur les cas d'usage, au besoin; 3) la participation des organisations autochtones et du Centre de gouvernance de l'information des Premières Nations aux prochaines phases du travail, y compris l'élaboration de normes. Du point de vue de la mise en œuvre, les organisations autochtones devront disposer des ressources nécessaires pour que leur participation soit significative.

Normalisation en action

La mise en œuvre et la mise à jour constante de cette feuille de route nécessiteront le travail constant d'un comité directeur et des membres du Collectif, en plus d'un financement continu servant à orienter, à organiser et à optimiser les activités de normalisation pour préparer le marché à l'essor de l'économie numérique.

À court terme, ce travail se traduira notamment par une surveillance continue du Collectif et de sa gouvernance, et par la communication et la promotion de la feuille de route auprès des intervenants. Un plan d'action pour les 35 recommandations sera préparé d'ici les deux premières années avec l'aide du Collectif.

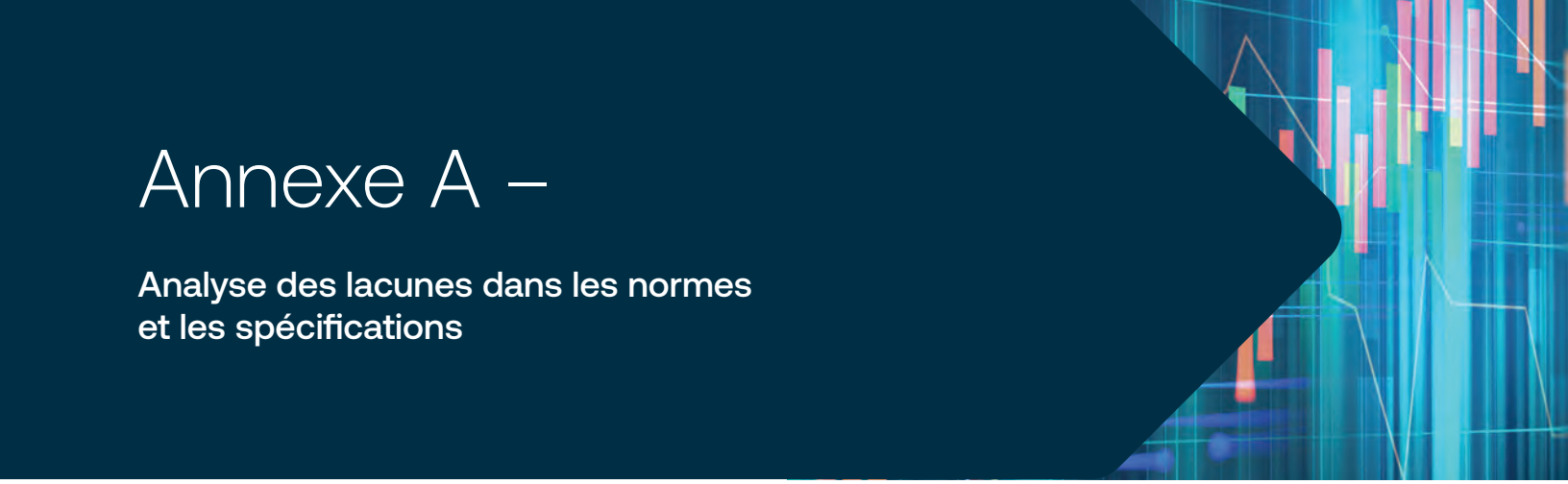
Le soutien de Statistique Canada permettra la création d'un tableau de bord pour suivre la mise en œuvre des recommandations et la résolution des lacunes cernées.

Grâce aux plans d'action, le Canada :

- deviendra un chef de file de l'élaboration des normes et un agent de changement à l'international dans la sphère de la gouvernance des données et des mégadonnées;
- dirigera la création de normes et de programmes d'évaluation de la conformité nationaux et internationaux;
- accroîtra sa participation et son influence au sein de comités d'élaboration des normes pertinents;
- conclura à l'international des ententes de normalisation qui appuient les politiques publiques et les priorités gouvernementales du Canada;
- fera progresser l'harmonisation et la cohérence d'une province et d'un territoire à l'autre;
- défendra la normalisation comme outil permettant l'atteinte d'objectifs réglementaires et économiques;
- fera la promotion de solutions de normalisation qui visent des secteurs en évolution et en émergence;
- favorisera et protégera la propriété intellectuelle d'entreprises canadiennes novatrices par la normalisation;
- se servira de leurs innovations et de leurs inventions pour élaborer des solutions de normalisation;
- protégera la santé et la sécurité des Canadiens grâce à des solutions de normalisation fondées sur la qualité, la confiance et l'éthique.

Voilà ce qui devrait mener à la création de normes et de programmes d'évaluation de la conformité internationaux qui participeront à promouvoir et à défendre les intérêts et les priorités des entreprises canadiennes, procurant par le fait même aux Canadiens plus de sécurité, de confidentialité et de contrôle relativement à leurs données et permettant une commercialisation sûre de ces dernières.

Nous entreprendrons une deuxième version de cette feuille de route en 2021 pour traiter d'enjeux qui n'ont pas été couverts dans la présente version et faire état de la progression de la mise en œuvre des recommandations.



Annexe A –

Analyse des lacunes dans les normes et les spécifications

La présente annexe contient : une description des principaux enjeux, avec les normes et les spécifications correspondantes, tant en vigueur qu'en cours de rédaction; des recommandations sur la nécessité de lancer de nouvelles activités de recherche et développement ou de créer de nouvelles normes et spécifications, ainsi que ce qu'il faut prioriser dans leur élaboration; et enfin les organisations qui pourraient s'en occuper. Le document se divise en plusieurs sections qui correspondent aux groupes de travail du Collectif canadien de normalisation en matière de gouvernance des données (CCNGD) : Fondements de la gouvernance des données; Collecte, organisation et classement; Accès, diffusion et conservation; et Analyse, solutions et commercialisation. À noter que les recommandations relatives aux organisations qui pourraient éventuellement se charger des travaux ne se veulent aucunement définitives ni classées par ordre de préférence ou d'autorité.

Groupe de travail 1 : Fondements de la gouvernance des données

Enjeu 1 – Cadre de responsabilité

Cet enjeu concerne la structure de responsabilité et de contrôle pour toutes les données créées ou recueillies ainsi que la définition des rôles et responsabilités en matière de traitement des données. La responsabilité du détenteur des droits sur les données, les conséquences d'un transfert de propriété et la notion de consentement ont également été abordées. L'objectif est de concevoir un cadre de responsabilité pour les chaînes d'approvisionnement en information des organisations. Ce cadre devrait comprendre les outils dont ont besoin ces organisations pour assurer leur conformité et leur transparence à l'égard des règlements sur les données. Et puisqu'il existe un vaste éventail de régimes de consentement possibles pour favoriser la transparence, il vaudrait mieux ne pas se limiter aux principaux formulaires privilégiés par les grands organismes. Les normes doivent aussi dissiper la confusion entourant la définition du consentement afin de mieux encadrer la gouvernance des données. Pour terminer, le cadre de responsabilité doit aborder les questions de gestion de l'identité et de traçabilité des données, tout au long du cycle de vie de l'information.

Or, l'absence de normes sur la gestion de l'identité et le consentement rend difficile la création d'un cadre de responsabilité rigoureux et nuit à l'élaboration de règlements. Il faudrait des outils pour gérer les questions de traçabilité et de responsabilité, puisque les utilisateurs ne savent souvent pas suffisamment d'avance à quoi serviront leurs données, à court comme à long terme. De plus, il sera très important d'harmoniser le processus de conception des normes et la réglementation pour faciliter la conformité et l'exécution. La manière d'appliquer le concept de consentement devra être claire. Enfin, il y a lieu de clarifier la différence entre le consentement implicite et le consentement explicite aux fins d'utilisation.

À noter que les écarts entre les différentes lois provinciales pourraient nuire à la création d'un cadre de responsabilité unique s'ils ne sont pas comblés. Il faudra déterminer comment les différents axes de responsabilité interagissent entre eux, par exemple en précisant dans quelles situations les provinces peuvent déclarer l'état d'urgence, pour mieux cerner les répercussions à l'échelle du Canada. C'était le cas dernièrement pour la crise sanitaire liée à la COVID-19, pendant laquelle la déclaration de l'état d'urgence par les provinces a eu un effet sur le contrôle et la réglementation des données. Cet événement constitue une occasion parfaite de revoir le système actuel pour améliorer les mécanismes de partage des données au pays. Il faudra donc des pratiques exemplaires et des lignes directrices pour améliorer la gestion des données dans l'intérêt public en temps de crise.

Lacune : Cadre de responsabilité. La recherche de normes a généré un grand nombre de résultats sur le sujet, mais très peu se sont avérés pertinents. La plupart se rapportent à un secteur particulier, principalement la santé et le transport, et la majorité ne traitaient du sujet qu'en partie. Fait intéressant : plus de la moitié des normes pertinentes datent de 2017 ou après, ce qui témoigne d'une volonté ferme de mettre en place les outils de normalisation nécessaires à une meilleure responsabilisation en gouvernance des données. La recherche n'a révélé aucune lacune évidente. La hausse des activités de normalisation entourant la responsabilité engendrera une gamme d'outils que pourront utiliser les organisations pour améliorer leur transparence à cet égard. Le plus difficile pour ces organisations sera de s'y retrouver parmi les règlements sur la protection des renseignements personnels émergeant dans les différentes provinces et d'harmoniser les normes à ces règlements.

Besoins en recherche et développement? Oui

Recommandation : Harmoniser les lois sur la sécurité et la protection de la vie privée au Canada, tout particulièrement dans le domaine du consentement.

Degré de priorité : Moyen

Organisation(s) : Bureau du directeur de l'information et commissariat à la protection de la vie privée dans les provinces et au fédéral

Enjeu 2 – Attestation encadrant les rôles professionnels

Cet enjeu concerne la clarification du rôle des professionnels qui traitent les données et l'information, les programmes d'attestation à créer et les besoins de l'industrie. Il s'agit d'abord d'évaluer les exigences en matière de compétences professionnelles en fonction d'un cadre clair qui formera la colonne vertébrale de la gouvernance des données. Ce cadre devrait tenir compte des besoins et de l'évolution rapide du secteur, et favoriser l'innovation plutôt que la ralentir. Vu l'importance de leur rôle, les professionnels des données ont un devoir envers la société. Il faudra donc étudier le rôle des associations professionnelles, dont les normes obligatoires auraient préséance sur les exigences des employeurs, pour prévenir les actes répréhensibles. L'objectif : protéger les organisations et les particuliers.

Monter un programme d'attestation pour un secteur novateur où les normes et les règlements sont rares n'est pas chose facile. Et il pourrait être difficile d'appliquer ce programme à un secteur aussi vaste et nouveau. Ce pourrait être nécessaire de concevoir un processus d'attestation propre aux différentes industries, en plus du processus général pour les données en tant que discipline (ex. : le processus d'attestation pour l'encodage des données sur la santé de l'Association canadienne interprofessionnelle du dossier de santé). Créer un code pour une profession en constante évolution comporte aussi son lot de risques, d'où l'importance d'établir un cadre avant d'élaborer des programmes d'attestation. L'application des normes et programmes d'attestation devrait être intégrée à la réglementation et faire l'objet d'un suivi pour éviter de créer un faux sentiment de sécurité. De même, les organisations se doivent de faire circuler leurs pratiques exemplaires et lignes directrices, pour les faire connaître aux gestionnaires et autres employés.

Il faudrait donner des présentations dans les écoles sur l'utilisation des données et les risques qui y sont associés, pour protéger les enfants et les jeunes adultes, groupes particulièrement vulnérables aux attaques. D'ailleurs, parallèlement à la formation professionnelle – de première importance –, les universités et les collèges devraient aussi proposer des programmes d'information pour assurer aux générations futures de travailleurs une compréhension générale du sujet. Ce courant de sensibilisation des jeunes aura un effet salutaire sur les pratiques des entreprises, pour le bien de la société.

Lacune : Attestation encadrant les rôles professionnels. La recherche de normes sur le sujet n'a généré qu'un petit nombre de stratégies normatives pour la qualification et l'attestation des organisations et professionnels. Très peu des normes se sont avérées pertinentes au domaine à l'étude. Ces résultats reflètent la difficulté d'élaborer des normes encadrant les rôles professionnels dans un secteur aussi évolutif, comme on l'explique ci-dessus. La recherche a aussi généré des normes sectorielles et des normes indirectement liées au sujet qui pourraient servir à la création de normes intersectorielles pour les professionnels des données. En conclusion, on constate un manque évident de normes sur la question, ce qui confirme la nécessité d'offrir aux professionnels des données un meilleur encadrement.

Besoins en recherche et développement? Oui

Recommandation : Concevoir des normes intersectorielles pour les professionnels des données.

Degré de priorité : Moyen/Faible

Organisation(s) : Data Management Association (DAMA), Association canadienne interprofessionnelle du dossier de santé (CHIMA), Digital Health Canada, Enterprise Data Management Council (EDMC), Healthcare Information and Management Systems Society (HIMSS), Association internationale des professionnels de la protection de la vie privée (IAPP)

Enjeu 3 – Habileté numérique

Cet enjeu aborde l'habileté numérique sous l'angle d'une meilleure compréhension des données, des technologies et des interfaces par la population canadienne. Il faut d'abord distinguer l'habileté numérique des attestations professionnelles, la première ayant une portée plus large qui s'étend à l'utilisation efficace et sécuritaire des technologies. L'éducation est un outil important pour sensibiliser les Canadiens aux difficultés et aux avantages d'une société de plus en plus numérique, ce qui servira à la mise en place d'un cadre de gouvernance des données efficace et inclusif. Au final, cette gouvernance est la responsabilité partagée de plusieurs, y compris le consommateur. Par exemple, les Canadiens devraient avoir les outils et les connaissances nécessaires pour reconnaître les fausses informations qui circulent sur le Web et comprendre le rôle de leurs données dans les analyses. Nous verrons aussi comment informer les gens, qui devrait s'en charger et quel est le rôle du gouvernement dans l'harmonisation de cette information à l'échelle du pays.

Il y a lieu de mieux coordonner les actions des organisations privées et des gouvernements pour synchroniser les efforts et éviter les dédoublements. Il faut des objectifs clairs pour éviter la confusion et assurer l'utilité et la fiabilité de l'information fournie. D'importants efforts devront être déployés pour informer et protéger les populations vulnérables et pour promouvoir l'adoption d'une approche inclusive de l'habileté numérique. L'évolution effrénée du domaine compliquera de beaucoup le maintien d'un niveau raisonnable d'habileté chez la population canadienne. Aussi le curriculum devra-t-il constamment être revu et retransmis.

Des programmes d'habileté numérique ont déjà commencé à faire leur apparition au Canada, pour l'enseignement des principes de base de la technologie aux enfants. Prenons par exemple celui du Yukon, appelé *Yukon Education Digital Literacy Framework*, qui aide les enseignants à transmettre aux élèves des compétences de base en technologie. Ce type d'initiative, qui a certainement sa place partout au Canada, peut être adapté aux différents groupes d'âge. D'ailleurs, les guides d'habileté numérique ne devraient pas se limiter aux établissements d'enseignement, mais pourraient être offerts à l'ensemble de la population, dans les médias ou les centres communautaires. L'idée est de démocratiser l'utilisation et la compréhension des technologies. Il faudrait aussi une meilleure collaboration entre le gouvernement et l'industrie dans l'offre de différents types de programmes pour différents secteurs. Par exemple, les organisations privées en santé ont déjà fait équipe avec le secteur universitaire et le gouvernement pour optimiser l'utilisation des technologies et des données dans le domaine; d'autres secteurs devraient reprendre l'idée. Des initiatives semblables se voient aussi en Finlande et ailleurs en Europe, comme la plateforme Elements of AI sur les principes de base de l'intelligence artificielle (IA).

Lacune : Habileté numérique. La recherche de normes dans ce domaine a donné très peu de résultats, même en tenant compte des normes indirectement liées au sujet et des normes sectorielles. Ce constat reflète la nouveauté de l'enjeu et le rôle grandissant de la société civile dans la gestion des données et des technologies. Les rares normes qui parlent de l'habileté numérique sont principalement destinées aux établissements jeunesse et pédagogiques, laissant pour compte une grande partie de la population. Le peu d'information dont dispose la société civile est très clairsemé et ne correspond pas aux besoins et aptitudes de la population active ou âgée. Cette lacune fait ressortir le besoin pressant de normaliser le tout pour protéger les groupes vulnérables des risques pour la confidentialité des données. Ce problème majeur nécessitera certainement une plus grande part de participation de la société civile aux activités de normalisation pour que les besoins particuliers de la population soient pris en compte.

Besoins en recherche et développement? Oui

Recommandation : Concevoir des normes accessibles aux différents segments de la société, par exemple les jeunes, les aînés et les personnes vulnérables.

Degré de priorité : Élevé

Organisation(s) : Ministères de l'Éducation des provinces et territoires, universités et collèges, médias, associations d'enseignants, ordre des enseignants (organisme de réglementation)

Enjeu 4 – Cybersécurité et protection des données

Cet enjeu couvre la cybersécurité, la protection des données et la transparence, éléments transversaux d'un cadre de gouvernance des données. Puisque les menaces évoluent en même temps que les outils technologiques, il nous faudra des mécanismes plus élaborés pour protéger les données et les renseignements confidentiels. Les principaux risques pour la cybersécurité concernent l'infrastructure numérique, de réseau et de connectivité. Par conséquent, il ne sera pas directement question de sécurité des technologies de l'information (TI), qui se rapporte plutôt à l'aspect matériel de l'infrastructure, bien qu'il y ait effectivement un lien étroit entre les deux domaines. Il y a également lieu de faire une distinction entre la sécurité des infrastructures, la sécurité du personnel et la responsabilité individuelle à l'égard de la cybersécurité, pour clarifier le rôle de chaque acteur[16].

Le premier obstacle à surmonter est l'incohérence des définitions sur la cybersécurité. Le grand nombre de normes sur le sujet empêche l'harmonisation à l'échelle nationale et internationale et l'adoption de règlements régionaux et nationaux cohérents. Conséquence : des inégalités dans les systèmes de cybersécurité des organisations, et donc des risques plus élevés pour les personnes vulnérables. Pour que la cybersécurité s'améliore, et pour inspirer confiance dans l'efficacité des mesures prises, il faudra aussi que le secret fasse place à la transparence. Il faut trouver l'équilibre entre transparence et confidentialité pour faire progresser la cybersécurité et éviter les dangers associés à une trop grande opacité.

De plus, des mesures de cybersécurité devraient être intégrées à toutes les nouvelles technologies. Effectivement, il est beaucoup plus facile de le faire à l'étape de la conception qu'après coup. Le gouvernement devrait en faire une priorité nationale, comme ce fut le cas dans l'Accord Canada–États-Unis–Mexique (ACEUM), qui tient compte du fait que les menaces à la cybersécurité peuvent nuire au commerce numérique. L'ACEUM invite également ses pays membres à envisager la cybersécurité du point de vue des risques plutôt que dans une optique de réglementation normative et à s'appuyer sur des normes consensuelles (paragraphe 19.15(2)). À cet égard, le Canada s'est doté d'un programme de certification en cybersécurité pour aider ses organisations à mieux gérer leurs mesures de protection. Cela dit, il reste beaucoup à faire pour harmoniser les normes et règlements à l'échelle du pays.

16 À ce sujet, voir l'article 4.7 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) (https://laws-lois.justice.gc.ca/fra/lois/P-8.6/page-11.html#h-417659), qui oblige les organisations à prendre des mesures matérielles, techniques et administratives pour protéger les renseignements personnels. La cybersécurité comprend donc, par exemple, la sécurité des salles de serveurs, les pare-feu et antivirus des systèmes et l'administration rigoureuse des privilèges d'accès à l'information en fonction des besoins. Il est impossible d'être plus précis, puisque la définition est appelée à évoluer en même temps que les risques en matière de cybersécurité. En gros, il faut se demander si la mesure employée est conforme au degré de confidentialité de l'information.

Lacune : Cybersécurité et protection des données. Un très grand nombre de normes ont été publiées sur le sujet. Une bonne partie se rapporte à un secteur donné, notamment les TI, le transport ou l'infrastructure. D'entre ces normes sectorielles, beaucoup portent sur la résilience et la sécurité de l'information. Fait intéressant : la grande majorité des normes jugées pertinentes datent d'après 2010, ce qui laisse croire à une hausse des activités de normalisation dans ce domaine au cours des 10 dernières années. À noter aussi que la plupart de ces normes ont trait à l'aspect de gestion des risques de la cybersécurité. Le paysage normatif fait ressortir le nombre considérable d'activités de normalisation en lien avec la cybersécurité, un bon signe, mais il sera important de miser davantage sur les solutions intersectorielles, qui ont été négligées.

Besoins en recherche et développement? Oui

Recommandation : Élaborer des normes intersectorielles.

Degré de priorité : Élevé

Organisation(s) : Organismes d'élaboration de normes (OEN) accrédités par le CCN

Enjeu 5 – Gouvernance de la gestion des données

Cet enjeu concerne la nécessité de planifier, de superviser, de surveiller et d'appliquer la gestion des données à l'échelle organisationnelle, ainsi que la manière de gérer ces données tout au long de leur cycle de vie. Cette gestion devrait couvrir l'élaboration, l'exécution et la supervision de plans, de politiques, de programmes et de pratiques visant à contrôler, à protéger, à assurer et à améliorer la valeur des données et des actifs d'information. Une bonne gouvernance devrait également prévoir un cadre qui permettrait l'examen de la gestion des données à l'échelle organisationnelle. En effet, l'adoption d'un système de gestion faciliterait la conformité aux règlements actuels et à venir. Ce système devrait donc s'inspirer principalement de la LPRPDE, avec des variations pour les différents règlements en vigueur partout dans le monde.

La portée et la définition du concept de gestion des données varient grandement selon les régions et les normes. En l'absence d'un consensus sur sa fonction, cependant, il est difficile pour les organisations de respecter les règlements sur le sujet. Il faut donc des règlements plus clairs pour encourager les organisations à gérer leurs données comme elles gèrent leurs actifs, ainsi que pour les tenir légalement responsables. Il nous faut étudier les pratiques exemplaires en place – directives, évaluations, outils, processus, etc. – pour en faire un cadre exhaustif. Chaque organisation pourrait ensuite adapter ce cadre général aux objectifs et aux besoins de son secteur. Le cadre de gestion des données devrait miser sur des objectifs de rendement plutôt que sur des règles prescriptives; cela faciliterait sa mise en œuvre et donnerait une meilleure marge de manœuvre aux organisations.

Chaque organisation devrait transposer ses objectifs dans sa politique de gestion des données, laquelle devrait être bien comprise de l'intendant (ex. : la politique de DAMA International, qui définit le rôle d'intendant des données). Il existe déjà différents modèles de gestion dans les grands organismes, comme le modèle d'évaluation des capacités de gestion des données (DCAM) de l'Enterprise Data Management Council (EDMC), qui utilise les pratiques exemplaires de l'industrie pour évaluer les capacités de l'organisation, de la phase stratégique jusqu'à la fin de la mise en œuvre. Ce modèle a été adopté par plus de 60 % des entreprises financières (y compris les cinq grandes banques au Canada). L'Institut canadien d'information sur la santé (ICIS) a aussi un cadre d'évaluation de la capacité qui compte quelques politiques et processus sur la gestion des données.

Lacune : Gouvernance de la gestion des données. Il existe quelques normes sur la gouvernance de la gestion des données à l'échelle organisationnelle et intersectorielle. Or, la plupart des normes qui ont un lien direct ou indirect avec le sujet ont été conçues pour un secteur donné ou se rapportent aux éléments matériels des systèmes plutôt qu'à la gestion du cycle de vie des données. De plus, la majorité des normes sectorielles se concentrent sur un aspect particulier du cycle de gouvernance, ce qui complique pour les organisations la création d'un cadre exhaustif. L'absence de normes couvrant l'ensemble des pratiques, politiques et contrôles internes entraîne à son tour un manque de mécanismes de gouvernance aux échelles intersectorielles et organisationnelles. Par contre, les nombreuses normes sectorielles pourraient servir de fondement pour la création de normes organisationnelles. En effet, plusieurs normes du domaine du transport, de la santé et de l'énergie peuvent être adaptées à d'autres secteurs.

Besoins en recherche et développement? Oui

Recommandation : Concevoir un cadre organisationnel de gouvernance des données adapté aux différentes tailles et aux différents types d'organisations.

Degré de priorité : Moyen

Organisation(s) : DAMA International

Enjeu 6 – Protection des renseignements personnels (enjeu regroupé avec celui des droits sur les données)

Cet enjeu concerne les renseignements personnels et leur contrôle. Il faut savoir que la définition et l'application des concepts de protection des renseignements personnels et de droits sur les données diffèrent grandement d'un règlement à l'autre. Aussi faut-il premièrement déterminer à qui reviennent les droits sur les données, si ces droits peuvent être cédés et qui peut diffuser les données. Le contrôle de l'information est un sujet de plus en plus pertinent, surtout maintenant que de nouvelles données peuvent être employées et générées par l'intelligence artificielle (IA) et l'Internet des objets. Les renseignements générés par ces nouvelles technologies devraient être aussi transparents, conformes et équitables que les autres, et leur diffusion consentie par le détenteur des droits. Les mesures de protection de l'information devraient être revues en fonction des règlements actuels sur les données, et des efforts s'imposent pour harmoniser ces règlements et normes et en faciliter l'application. Par exemple, la *Charte canadienne du numérique* devrait être revue en fonction des normes et règlements internationaux. La *Charte canadienne des droits et libertés* devrait servir de guide, puisque le tout tombe dans la catégorie des droits sur les données.

Les concepts de détention des droits et de contrôle sont à clarifier en ce qui touche la protection des renseignements personnels et la transparence. Par exemple, la cession des droits, si elle se fait par consensus, devrait être mieux réglementée et plus transparente pour protéger le détenteur initial des droits. Le concept de droits ne s'applique pas aux données comme il s'applique aux autres biens, et encore moins quand plusieurs parties ont joué un rôle dans la création de ces données. Il faut alors se demander comment les droits devraient être répartis. Même quand les données ont un propriétaire désigné, ces droits ne définissent pas ce que le propriétaire peut en faire. D'ailleurs, il pourrait être nécessaire de contourner temporairement certains droits en cas d'urgence.

Le contexte devrait-il avoir un effet sur l'application des droits sur les données et le contrôle de ces données pour le bien commun? Les circonstances dans lesquelles le gouvernement accède aux renseignements des citoyens et déroge aux droits établis doivent être revues. Le détenteur des droits devrait-il pouvoir refuser cet accès? Certes, les temps de crise exigent des mesures gouvernementales exceptionnelles, mais il faut des critères clairs pour ce qui doit se passer après la crise. De même, si les données doivent être communiquées à une organisation privée (ex. : une compagnie pharmaceutique en temps de crise sanitaire), il faudrait prévoir des mécanismes pour garantir leur suppression des bases de données de cette organisation une fois la crise passée. La définition des rôles des différents acteurs de la gouvernance des données et de la portée de leurs droits respectifs devrait contribuer à lever certaines ambiguïtés.

Lacune : Protection des renseignements personnels. Ce sujet a généré un grand nombre de normes, surtout en ce qui concerne la communication de données dans les secteurs de la télécommunication et des TI. Une grande part des normes ont été jugées pertinentes, ce qui confirme l'importance grandissante accordée à la protection des renseignements personnels dans les 10 dernières années. La recherche de normes a également fait ressortir des progrès en protection des renseignements et en confidentialité dans le secteur de la santé; beaucoup de normes traitent de ces questions. Toutefois, il semble manquer de normes relatives aux droits sur les données et à la gestion de ces données, deux domaines problématiques relevés ci-dessus. Pour terminer, même si un certain travail de normalisation a été entamé pour encadrer les technologies émergentes, comme l'IA, les chaînes de bloc et les mégadonnées, il semble toujours manquer de normes dans ce domaine.

Besoins en recherche et développement? Oui

Recommandation : Harmoniser les lois sur la vie privée et la sécurité du Canada, notamment dans le domaine du consentement.

Degré de priorité : Élevé

Organisation(s) : Bureau du directeur de l'information et commissariat à la protection de la vie privée dans les provinces et au fédéral

Enjeu 7 – Directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique

Cet enjeu concerne la fiabilité et l'éthique dans l'utilisation des données, par rapport aux attentes canadiennes en matière de renseignements personnels énoncées dans la *Loi sur la protection des renseignements personnels et les documents électroniques* ainsi que dans la *Loi sur la protection des renseignements personnels*. Il consiste à clarifier les aspects éthiques de la propriété ou de l'intendance des données, ainsi que leur utilisation éthique et sociale en fonction de leur valeur publique. Il faudrait mieux comprendre ce qu'il faut aux propriétaires, aux intendants et aux fournisseurs de données ainsi qu'au public pour être dignes de confiance dans la collecte, la gestion, la conservation et l'utilisation de ces données, et pour démontrer activement leur fiabilité tout au long du cycle de vie des renseignements. La question de l'éthique couvre aussi les circonstances extrêmes où certaines mesures de protection devraient être levées ou modifiées. (Ex. : En ces temps de pandémie, quels sont les obstacles à la collecte, au partage et à l'utilisation éthique des données dans le domaine de la santé?) Il sera aussi question de la nécessité d'élaborer des pratiques d'éthique propres aux différents secteurs.

Encadrer la fiabilité, le traitement éthique et l'utilisation publique des données tout au long de leur cycle de vie est loin d'être facile. Il faudra répondre à une multitude de questions pour assurer la sécurité des renseignements. (Ex. : Quelles données faut-il recueillir? Qui devrait y avoir accès? Quel point de vue faut-il adopter dans l'analyse des données? Quels sont les principes éthiques à respecter dans le choix de ce point de vue?) Le grand nombre d'intervenants et le transfert des données d'une application à l'autre compliquent le suivi de l'utilisation des données. Sans mécanismes régulateurs et sans transparence pour éviter les actes répréhensibles, il y aura toujours des risques. Par exemple, le suivi des déplacements d'une personne au moyen de son téléphone pour des raisons de santé (ex. : pendant la pandémie de COVID-19) risque d'entraîner un usage mal intentionné de ces données. D'ailleurs, les méthodes numériques de recherche des contacts posent divers problèmes d'éthique en lien avec la protection de la vie privée, le consentement, l'autonomie, l'équité, l'accessibilité, etc. Décentraliser le contrôle des données et l'accès à ces données pourrait faire partie de la solution pour améliorer la fiabilité des données (un modèle déjà appliqué dans le domaine de la santé).

Il existe déjà de nombreux cadres sur la fiabilité et l'utilisation éthique des données, comme les normes de l'Institute of Electrical and Electronics Engineers (IEEE) et du ISO/IEC JTC 1/SC, mais il serait peut-être bien d'harmoniser les définitions et cadres proposés par les différentes organisations. Il existe aussi des lois, comme la *Loi sur la protection des renseignements personnels* et la *LPRPDE*, qui réglementent la question. Cela dit, il semble falloir d'autres lois et instruments pour bien encadrer les questions de consentement et de transparence. Ce sera essentiel pour assurer l'utilisation acceptable des données par l'industrie et le gouvernement. En effet, il arrive partout dans le monde que des entités politiques utilisent à tort des données sans le consentement de leurs citoyens. Il y a donc d'importants risques politiques à prendre en compte.

Lacune : Directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique. Le sujet étant assez large, il a généré un grand nombre de normes, mais la plupart n'en traitent qu'indirectement ou se rapportent à un secteur donné. Les normes sectorielles portent plus sur les questions d'environnement et de transport que sur l'utilisation des données. De plus, la plupart des normes sur le sujet sont très clairsemées et ne semblent pas définir en détail les responsabilités de tous les intervenants dans le cycle de vie des données. Comme on l'explique ci-dessus, un des principaux facteurs de cet enjeu consiste à assurer la fiabilité des données d'un intervenant à l'autre tout en veillant à l'utilisation éthique pendant toute la durée du cycle de vie. D'ailleurs, plus de la moitié des résultats de la recherche étaient en lien avec la collecte, et très peu touchaient aux autres aspects du cycle de vie. Toutefois, il est intéressant de noter que plus d'un tiers des normes analysées pour cet enjeu dataient de 2015 ou après, ce qui témoigne d'un grand courant de normalisation sur le sujet.

Besoins en recherche et développement? Oui

Recommandation : Concevoir des normes qui couvrent plus exhaustivement les responsabilités de tous les acteurs dans le cycle de vie des données.

Degré de priorité : Moyen/Faible

Organisation(s) : OEN accrédités par le CCN et OEN internationaux

Enjeu 8 – Données ouvertes et procédures d'harmonisation et d'interopérabilité des données

Cet enjeu couvre l'harmonisation des pratiques relatives aux données ainsi que les rapports entre la technologie, les processus et les systèmes. Il y est aussi question de l'utilité des pratiques stratégiques, légales et commerciales pour faciliter l'interaction entre entreprises et industries. On parle donc, plutôt que de pratiques techniques, d'interopérabilité au sens général, plus particulièrement de la possibilité de transférer des données d'une plateforme à une autre avec le plus de précision et le moins d'interventions possible, tout en assurant la sécurité et la confidentialité des renseignements. Le concept d'interopérabilité reste cependant à définir en fonction de l'industrie, du contexte et de la gouvernance. Il y a lieu de comparer l'intérêt des régimes rigides et des régimes flexibles aux fins stratégiques et opérationnelles. L'infrastructure de données ouvertes, qui permet à des tiers d'accéder aux données, sera également abordée.

Il existe un réel besoin de définir et de promouvoir les pratiques d'interopérabilité, qui ne consistent pas à donner à des acteurs externes accès aux données, mais plutôt à faciliter l'échange d'information quand c'est nécessaire. Pour ce faire, il faut étudier la question sous de nombreux angles, à commencer par l'uniformisation du format des champs de date dans les modalités de service, ce qui peut occasionner d'importantes complications. Bien qu'il existe déjà plusieurs normes pour l'interopérabilité et l'harmonisation des pratiques relatives aux données, celles-ci restent peu utilisées. Il faudrait mieux les intégrer dans les règlements pour favoriser leur utilisation et faciliter l'adoption de bonnes pratiques commerciales à l'échelle des entreprises et des administrations. Cela dit, des considérations politiques pourraient nuire à cette initiative d'harmonisation.

L'interopérabilité touche des aspects différents de différentes industries. Par exemple, dans le secteur de la santé, les données de diverses sources sont rapidement intégrées pour assurer la prestation de soins de santé de qualité, ce qui nécessite l'adoption de pratiques et politiques harmonisées pour évaluer les besoins en interopérabilité du système de santé. Ce secteur s'est aussi donné des limites et critères clairs quant aux données qui devraient ou non être interopérables pour protéger la vie privée des patients. Dans d'autres secteurs, comme celui des finances, les dernières années ont vu une transition générale vers les normes ISO (ex. : ISO 8583 et 20022). À terme, l'industrie devrait recourir plus souvent aux normes pour fournir aux clients des données personnelles qui seront déjà interopérables.

Lacune : Données ouvertes et procédures d'harmonisation et d'interopérabilité des données. Une bonne part des normes trouvées portent effectivement sur le sujet, ou du moins en partie, ce qui révèle la tenue d'importantes activités de normalisation visant à améliorer l'uniformité et les pratiques de gouvernance des données dans les dernières années. En effet, plus de 90 % des normes pertinentes datent des cinq dernières années. De plus, ces normes ont presque exclusivement été élaborées à l'échelle internationale par des OEN comme l'Organisation internationale de normalisation (ISO), la Commission électrotechnique internationale (IEC) et le Secteur de normalisation des télécommunications de l'Union internationale des télécommunications (UIT-T), ce qui facilite l'harmonisation entre les pays. Il est intéressant de remarquer le peu de normes sectorielles, ce qui pourrait refléter un désir des professionnels des données des différents secteurs d'uniformiser leurs pratiques. Il ne semble donc pas avoir de grandes lacunes dans les domaines de l'harmonisation et des pratiques de gouvernance des données, grâce à une foule d'activités de normalisation. Toutefois, il sera important d'intégrer rapidement les nouvelles pratiques aux discussions sur les normes.

Besoins en recherche et développement? Non

Recommandation : Rester proactif en ce qui a trait à l'harmonisation et à l'interopérabilité des nouvelles pratiques et technologies.

Degré de priorité : Moyen/Faible

Organisation(s) : OEN accrédités par le CCN et OEN internationaux

Enjeu 9 – Rôles des acteurs et des opérations en matière de traitement des données

Cet enjeu couvre le rôle des différents acteurs qui participent au cycle de vie de la chaîne d'approvisionnement. De la collecte à l'utilisation des données interviennent une multitude de processus de traitement. Peu importe la quantité de données, de nombreuses personnes sont impliquées, qu'il s'agisse de les protéger contre les accès non autorisés ou de faire des sauvegardes quotidiennes, par exemple. Ces acteurs sont responsables de protéger les données en créant un système sécurisé qui réduit les risques d'erreurs. L'enjeu souligne donc la responsabilité des professionnels des données et leurs obligations. Il y a également lieu d'étudier, d'entre les différents modèles de responsabilisation, lequel est le plus efficace (ex. : responsabilité personnelle ou professionnelle).

La rareté et l'incohérence des règles sur la gouvernance en matière de contrôle et de responsabilité des données entravent grandement l'utilisation responsable de ces données par les professionnels. La création d'associations de professionnels des données, qui veilleraient à la conformité de leurs membres en leur retirant leur attestation en cas de manquements répétés, pourrait être un excellent moyen de compenser le manque de règlements clairs. D'autre part, le traitement de l'information se complique de plus en plus et nécessite toujours plus d'acteurs au cours de son cycle de vie, ce qui peut rendre difficile le respect de lois ou de contrats dont les dispositions ou la validité peuvent changer en fonction de l'endroit. Il importe donc plus que jamais de définir les opérations et les acteurs du cycle de vie des données. L'utilisation d'algorithmes nécessite aussi la création de mesures de responsabilisation, de normes et de programmes d'attestation pour en assurer la conformité.

La montée de la technologie et de la collecte des données dans les différents secteurs a créé une multitude de rôles liés à l'information qui doivent maintenant être définis et supervisés par un organisme central. Des listes des rôles ont déjà été dressées pour certains secteurs, comme celui des finances par l'Enterprise Data Management Council (EDMC). Il existe également des cadres plus généraux, comme le Cadre de confiance pancanadien, qui favorisent l'utilisation sécuritaire et le traitement confidentiel des données et devraient s'appliquer à tous les secteurs. Pour améliorer la conformité, il serait bon de promouvoir ces cadres dans les différents règlements. Quant à la prise de décisions automatisée et à l'utilisation d'algorithmes, le gouvernement du Canada a publié la *Directive sur la prise de décisions automatisée* ainsi que l'outil d'évaluation de l'incidence algorithmique, pour l'évaluation et l'atténuation des conséquences du déploiement d'un tel système.

Lacune : Rôles des acteurs et des opérations en matière de traitement des données. La recherche a généré une longue liste de normes non pertinentes et de normes propres à des secteurs tels que le transport et les télécommunications. Fait intéressant : la plupart des normes sectorielles portaient sur les rôles, les chaînes d'approvisionnement et les opérations de traitement des données, tandis que les normes jugées pertinentes portaient davantage sur la responsabilisation. Cette distinction est parlante, car elle montre l'utilité des normes sectorielles pour répondre aux besoins particuliers des professionnels des données. Il serait certainement profitable d'utiliser ces normes, dont plus de 85 % datent d'après 2010, comme fondement pour la création de normes intersectorielles, très rares pour le moment, et ainsi faciliter la supervision des professionnels des données sur l'ensemble des secteurs.

Besoins en recherche et développement? Oui

Recommandation : Créer des normes intersectorielles.

Degré de priorité : Élevé

Organisation(s) : ISO/IEC, OEN accrédités par le CCN

Enjeu 10 – Réutilisation des données

Cet enjeu porte sur la réutilisation des données, c'est-à-dire leur utilisation à d'autres fins que celles auxquelles elles ont été recueillies ou consenties explicitement par le détenteur des droits sur les données. Dans ces cas, l'avis de consentement devrait expliquer clairement à quoi serviront les données et les limites de cette utilisation pour éviter tout différend entre le détenteur des droits et l'utilisateur des données, comme l'exige la loi. On verra aussi la possibilité de supprimer les données et de retirer un consentement. Il faudra déterminer quand se termine le consentement. Par exemple, expire-t-il lors du décès d'un patient hospitalisé ou de la fermeture d'un compte bancaire? Enfin, il sera important de voir si des directives sur l'anonymisation des données s'imposent et quel rôle pourrait jouer cette anonymisation.

La réutilisation pose problème si le propriétaire des données ne consent pas explicitement à l'usage visé par l'utilisateur. Autrement dit, il faudrait décrire explicitement chaque étape de l'utilisation dans les formulaires de consentement. Cette précaution pourrait aussi éviter la monétisation non autorisée des données. On remarque que le fait d'aborder la réutilisation des données en deux parties, soit l'accès aux fins de consultation et l'accès aux fins de modification, pourrait réduire les utilisations répréhensibles. Par exemple, les intendants des données sont autorisés à consulter et modifier l'information, puisqu'ils peuvent être appelés à la corriger, tandis que les analystes et les scientifiques des données ont seulement besoin de consulter l'information pour l'analyser.

Parfois, la réutilisation des données sert à améliorer le fonctionnement de certains secteurs, ce qui profite grandement au consommateur. Dans le domaine financier notamment, elle est nécessaire à la communication des antécédents aux agences d'évaluation du crédit ou autres institutions financières. De même, dans le domaine de la santé, les données anonymes et regroupées servent à l'élaboration des politiques et à l'amélioration des processus. Si les données servent à d'autres fins que celles initialement autorisées, il est alors important d'en informer correctement le détenteur des droits et d'obtenir son consentement explicite par un moyen transparent et sécurisé.

Lacune : Réutilisation des données. La recherche de normes sur le sujet n'a donné qu'un petit nombre de résultats pertinents. La plupart d'entre eux semblent traiter la question sous l'angle de l'accès aux données; très peu de normes pertinentes se concentrent sur le consentement, problème principal relevé pour cet enjeu. De plus, environ la moitié des normes sur le sujet relèvent d'un secteur en particulier, comme la santé, le transport ou l'électricité. Un grand pourcentage de ces normes sectorielles se concentrent sur la traçabilité des données; très peu traitent du consentement. On constate donc un besoin général de normes intersectorielles visant principalement le consentement à la réutilisation des données. Cela dit, il est important de noter que la majorité des normes pertinentes sont assez récentes, ce qui laisse croire que plusieurs activités de normalisation pourraient déjà être en cours pour répondre à ce besoin.

Besoins en recherche et développement? Oui

Recommandation : Concevoir des normes sur l'obtention du consentement et la protection du détenteur des droits sur les données.

Degré de priorité : Moyen

Organisation(s) : Institut canadien d'information sur la santé (ICIS)

Groupe de travail 2 : Collecte, organisation et classement

Enjeu 11 – Collecte des données

Cet enjeu concerne la collecte primaire de données que font les organisations publiques et privées, à leurs propres fins. Il englobe le processus avant collecte de même que la collecte en soi. Pour cette dernière, on constate la nécessité de trouver un équilibre entre l'utilité des données et les moyens employés pour les obtenir. Les groupes de données ainsi que d'autres facteurs, comme la fréquence et les outils de collecte (formulaires, interface de passage des messages [MPI], moissonnage du Web, téléphone, etc.), devraient aussi être pris en compte lors de l'ajout, de la manipulation, du nettoyage et du regroupement potentiel des données. Quant au processus avant collecte, il comprend la possibilité de repérer les besoins et de trouver des données semblables déjà recueillies.

Il faudrait faire la liste des normes portant déjà sur la collecte de données de diverses sources – détection géospatiale, capteurs, sondages ou Web – et voir si l'on peut s'en servir pour détecter et évaluer les lacunes relatives à d'autres types de données. Les sources de données peuvent être divisées en trois grandes catégories : 1) les données analogiques, c'est-à-dire qui sont recueillies et gérées à l'ancienne; 2) les données numériques, c'est-à-dire qui viennent d'une source statique, mais qui peuvent être recueillies, stockées, manipulées et traitées électroniquement; et 3) les données dynamiques en continu, c'est-à-dire qui viennent de l'Internet des objets, de capteurs, etc.

L'analyse s'est également penchée sur la consignation des attributs des données – les métadonnées – aux fins d'évaluation de la qualité. Comme l'a illustré la pandémie de COVID-19, la représentativité et l'inclusivité des données, particulièrement quand elles se rapportent à des groupes de la population, sont extrêmement importantes. Ces « principes » de collecte font donc partie de l'enjeu. Il serait aussi nécessaire de veiller à pouvoir dégrouper les données selon le sexe, l'âge et la province ou le territoire pour tenir compte des disparités au sein de la population. L'évaluation de la crédibilité du fournisseur de données est aussi un élément essentiel de cet enjeu.

Lacune : Collecte des données. La recherche a généré un grand nombre de normes à ce sujet, dont 20 % correspondant au niveau I ou II. La plupart des normes les plus pertinentes portent sur la collecte par les appareils de l'Internet des objets (série Y du Secteur de normalisation des télécommunications de l'UIT). La norme générique ISO 8000 sur la qualité des données encadre en partie la collecte, de même que la norme ISO 14048, sur l'analyse du cycle de vie et le format de documentation de données. La collecte de données satellite en fait aussi partie. Pour les autres aspects de cet enjeu, il semble y avoir de nombreuses normes, mais la vaste majorité d'entre elles se rapportent très précisément à un type de donnée ou à une utilisation particulière. Ces normes spécifiques pourraient servir de fondement à une norme plus générique, mais pour le moment, on remarque des lacunes dans les domaines du processus avant collecte, de la collecte et de la consignation des attributs.

Besoins en recherche et développement? Non

Recommandation : Élaborer des normes par groupe de catégories de données afin d'assurer la cohérence des règles pour chacun de ces groupes. Le contexte de la COVID-19 illustre bien l'utilité des normes sur la collecte de renseignements sur la santé, mais il n'est peut-être pas possible d'établir une seule norme pour tous les types de données.

Degré de priorité : Élevé

Organisation(s) : OEN accrédités par le CCN

Enjeu 12 – Gestion des systèmes de données

Cet enjeu concerne la gestion des systèmes de données, y compris des programmes, logiciels, algorithmes, règles et politiques de gestion des données. L'analyse a porté sur les questions d'interopérabilité et de sécurité (pour les technologies de l'information). D'ailleurs, il manque de normes dans le domaine de la sécurité, plus précisément du chiffrage et des contrôles d'accès. Les normes sur le chiffrage, le marquage et l'authentification des données ont aussi été abordées, de même que la nécessité d'assurer la qualité des données par l'adoption de mesures de sécurité.

Également à l'étude : l'importance de la communication entre les mécanismes et appareils pour assurer l'interopérabilité des données. Il y a lieu de réfléchir aux exigences minimales pour le téléchargement de données dans un système, selon les besoins de celui-ci. À noter que la gestion des systèmes de données dépend en partie du cycle de vie du système, qui passe par la conception, l'élaboration, la mise à l'essai, le lancement, la maintenance ou le soutien technique et le retrait. Elle dépend aussi du type de système (regroupement, administration ou collecte) plutôt que du type de données. Tout système qui traite de l'information doit être régi par des stratégies et des règles de gouvernance.

Pour terminer, il faudrait clarifier si la gestion des systèmes dépend du type de données hébergées et s'il faut différents groupes de normes pour l'encadrer. Par exemple, on pourrait considérer cette gestion comme une application servant à intégrer, manipuler et supprimer des données. Se pose aussi la question de savoir si les normes sont appliquées à toutes les opérations ou étapes du cycle de vie des données.

Lacune : Gestion des systèmes de données. D'après les résultats de la recherche de normes, il semble y avoir des manques dans la plupart des aspects de cet enjeu. Les résultats se rapportent principalement à la gestion des données plutôt que des systèmes de données, l'objet réel de cet enjeu. Beaucoup des normes portent sur la gestion de l'accès. Les mots clés « gestion des systèmes d'information » ont donné des résultats pertinents, mais dans des domaines précis (ex. : secteur public ou circulation aérienne). La question reste : la gestion des systèmes de données dépend-elle du type de données? Faut-il concevoir des groupes de normes différents pour en tenir compte? Aucune norme ne visait le cycle de vie ou les stratégies de gouvernance des systèmes.

Besoins en recherche et développement? Non

Recommandation : Élaborer des normes sur le sujet, possiblement par groupe de types de données.

Degré de priorité : Faible

Organisation(s) : DAMA international

Enjeu 13 – Visibilité des données

Cet enjeu concerne la visibilité des données, c'est-à-dire la mesure dans laquelle les utilisateurs savent qu'une source ou un jeu de données existe, comment le trouver et comment l'utiliser. Pour les attributs et les métadonnées par exemple, il s'agit d'avoir l'information nécessaire pour ensuite évaluer son adéquation à un programme ou une activité. Un élément clé de cet enjeu réside dans la distinction entre la possibilité de trouver l'information et celle d'y accéder. Le cadre actuel dit à peu près la même chose : l'accès aux données ne garantit pas que ces données peuvent être « saisies et utilisées ».

Bien que le traitement, l'analyse, le couplage et l'interprétation des données n'entrent pas dans l'enjeu de la visibilité et de l'accès, le rôle des inventaires ou catalogues dans la recherche devrait être pris en compte dans la définition du sujet à l'étude. Faudrait-il un registre ou un système d'extraction? Et le fonctionnement de ce système devrait-il être abordé dans les normes? L'analyse s'est également penchée sur les moyens de motiver les gens à alimenter et entretenir le système, et sur la nécessité de proposer une norme pour la taxonomie des données disponibles.

Enfin, on a abordé l'importance de savoir comment les données sont interprétées, numérisées, recueillies et formatées. Le suivi des méthodes d'interprétation et d'analyse est vital au couplage des informations. Il faut aussi tenir compte des besoins en protection des données pour déterminer quelles informations devraient être faciles à trouver et lesquelles devraient rester cachées. La gestion des droits et privilèges d'accès devrait faire l'objet d'une étude, puisque des métadonnées protégées dans un certain système pourraient être retirées et transformées en données réelles ailleurs. En effet, les métadonnées correspondent à une étape du cycle de vie où elles peuvent se transformer en données réelles à mesure des transferts. Il reste à déterminer le rapport entre les règlements sur la protection de la vie privée et la visibilité des données. Certaines données doivent être visibles pour des raisons réglementaires ou légales, mais il est aussi nécessaire de protéger les renseignements confidentiels, comme les mots de passe. Citons en exemple le cas des journalistes en zones de guerre dont les photos pourraient être prises et utilisées par différents acteurs.

L'absence de définitions claires et cohérentes est un problème à corriger dans les normes sur la visibilité des données. C'est particulièrement vrai des métadonnées, terme aussi utilisé pour décrire les attributs des données recueillies. Par exemple, une norme sur les stations météorologiques en cours de rédaction par l'Association canadienne de normalisation (CSA) décrit les attributs de ces stations, comme les capteurs, les méthodes de transmission des données, la fréquence et les systèmes de management de la qualité pour la collecte et la transmission, pour donner aux utilisateurs une idée des caractéristiques de la collecte, et donc du type de données auxquelles ils accèdent. De plus, les normes actuelles et les besoins en nouvelles normes peuvent varier selon le type de données. Par exemple, on ignore s'il existe des normes ouvertes qui s'appliqueraient à l'ontologie particulière et exclusive de moteurs de recherche comme ceux de Google et d'Apple. En revanche, dans le domaine de la compilation ponctuelle de données géospatiales, les données à venir ne peuvent pas encore être assurées, mais la structure de ces données est déterminée avant leur création. Le rôle de l'apprentissage machine ou de l'IA dans la visibilité des données a été étudié. Il importe de déterminer s'il existe des pratiques exemplaires et des outils de recherche ou de détection qui pourraient nous en apprendre plus sur la recherche automatisée et les algorithmes d'IA, d'apprentissage machine ou d'interface de programmation d'applications.

Lacune : Visibilité des données. La recherche de normes a généré plus de résultats correspondant aux niveaux I et II pour ce sujet – 45 % – que pour les autres sujets abordés par le groupe de travail. Certains de ces résultats rejoignent des éléments d'autres enjeux, comme l'accès aux données (enjeu 21), ainsi que les métadonnées et l'utilisation d'une taxonomie standard (enjeu 41). En ce qui concerne la disponibilité des métadonnées, en soi ou pour la recherche de données, il existe des normes pour des formats, langues ou industries donnés. Il y a également quelques normes génériques sur la visibilité des données, comme la norme IEEE 2413, *An Architectural Framework for the Internet of Things (IoT)*, la norme ISO/IEC 19763-1, *Technologies de l'information – Cadre du métamodèle pour l'interopérabilité (MFI)*, ou la norme ISO/IEC TR 20943-1, *Technologies de l'information – Procédures en vue d'obtenir la cohérence du contenu d'un registre de métadonnées*, qu'il faudrait étudier pour savoir si les éléments soulevés par le présent enjeu sont couverts ou s'il s'agit d'une lacune importante à combler.

Besoins en recherche et développement? Non

Recommandation : Concevoir une norme exhaustive sur la visibilité des données.

Degré de priorité : Élevé

Organisation(s) : OEN accrédités par le CCN

Enjeu 14 – Couplage des informations

Cet enjeu concerne le couplage des informations, c'est-à-dire le fait de combiner les données sur une personne physique ou morale avec celles d'au moins une autre source pour enrichir un jeu de données. Il recoupe les enjeux de consentement et de sécurité, puisque les données ne viennent pas du même endroit, mais cette méthode comporte certains avantages en matière de confidentialité. De ce point de vue, le couplage constitue davantage un modèle conceptuel adapté aux besoins. Les questions de sémantique, de métadonnées et d'ontologie sont alors importantes, car le couplage peut donner lieu à des métadonnées ou des regroupements logiques selon les domaines.

L'éthique du couplage dépend de la visée initiale de la collecte. Autrement dit, l'information peut avoir été couplée pour une raison autre que celle énoncée à la collecte, d'où l'intérêt du couplage, ce qui peut avoir des répercussions sur la protection de la vie privée. Il arrive que le couplage de points de données indépendants dévoile l'identité de la personne concernée par les renseignements. Le couplage doit donc avoir un but très précis, acceptable et avéré. Il faut préciser que les couplages ne constituent pas des données organisées officiellement dans l'organisation. Ainsi, il est possible de les consigner, même s'ils comprennent des renseignements sur des personnes, puis de regrouper ces informations. Le terme « couplage de données » dans le contexte de cet enjeu s'utilise au sens général de liaison de deux fichiers. La différence entre le couplage et la traçabilité, soit l'acte de définir la portée, le sens et les processus des données, a aussi été étudiée. Il reste à présent à explorer la relation entre le couplage et l'éthique pour définir les normes à adopter. De plus, il faudrait étudier les aspects éthiques de la gouvernance et des motifs du couplage. En ce qui concerne les mécanismes, il y a lieu de voir les effets du couplage sur les questions d'éthique et de sensibilité, notamment à savoir s'il faut envisager différents mécanismes selon le degré de sensibilité des données.

Il faut des normes et lignes directrices sur le regroupement de données, pour traiter à la fois des aspects philosophiques et techniques de l'enjeu, de même qu'un mécanisme d'évaluation de la qualité des couplages. La protection et l'élimination des données d'origine ainsi que les questions éthiques entourant le couplage restent à voir. Par exemple, la collecte des données pourrait être vue dès le départ plutôt qu'à l'étape du regroupement. Par ailleurs, il est essentiel de déterminer comment contrôler, et ainsi assurer, la qualité des données issues de la science citoyenne ou de différentes plateformes. Étant donné les risques pour l'interopérabilité sémantique qui découlent des incohérences dans les formats et l'interprétation des couplages, il importe que le couplage contribue à la qualité des données. Or, il n'existe aucune ontologie sémantique générale. On remarque aussi un manque de modèles conceptuels et une réticence à adapter un modèle existant, car le travail sur ces modèles comporte son lot de risques.

Lacune : Couplage de données. D'entre tous les enjeux, la recherche de normes sur ce sujet a été la plus fructueuse. Malheureusement, la vaste majorité des résultats recoupent d'autres enjeux et ne se limitent pas au contexte décrit ci-dessus. Par exemple, les références relatives aux attributs, à la sémantique et à la qualité des données traitent de ces domaines en des termes plus généraux que ceux du couplage des données. Les aspects de consentement, de confidentialité et de protection de la vie privée sont cependant bien décrits dans une norme concernant les renseignements sur la santé. Le cadre technique sur la gestion des renseignements personnels dans l'Internet des objets semble aussi en parler. Hors du secteur de la santé, il semble y avoir un manque criant de normes sur le couplage des données. À noter que la question a été traitée en 2017 dans le projet de loi 87 de la Saskatchewan sur les ententes de couplage des données.

Besoins en recherche et développement? Non

Recommandation : Quoique certaines normes traitent en partie du couplage des données, elles ne couvrent pas suffisamment l'ensemble du sujet. Il faudrait donc une norme couvrant la totalité du processus, y compris la nécessité de faire approuver le couplage ou d'informer les personnes concernées.

Degré de priorité : Moyen/Faible

Organisation(s) : OEN accrédités par le CCN

Enjeu 15 – Marquage manuel des données

Cet enjeu concerne le marquage des données, qui consiste à condenser les données en codes précis et à les normaliser. Les normes sur les codes pour les médias sociaux ont entre autres été étudiées, ainsi que la reconnaissance faciale, un aspect important de cet enjeu. Puisque les systèmes d'IA utilisent des algorithmes différents des modes de pensée humaine, le marquage manuel pourrait servir à corriger les erreurs commises par l'IA et aurait priorité sur ces algorithmes automatisés. La combinaison d'IA et de corrections manuelles donnerait de meilleurs résultats que l'une ou l'autre de ces méthodes séparément.

Il faudrait savoir s'il existe des normes sur les systèmes de cotation du marquage ou des pratiques exemplaires qui pourraient en améliorer la fiabilité. Quant au marquage manuel, un récent article de presse rapporte que la Chine a déposé une proposition d'étude nouvelle (NWIP)[17] auprès de l'Union internationale des télécommunications (UIT) concernant la reconnaissance faciale, et que la portée et la taille de la norme proposée n'ont pas plu aux participants européens et américains de ces comités. Il y a lieu de se pencher sur la question, car elle implique la possibilité que des entités uniques s'approprient la définition d'une sous-catégorie de métadonnées. Les règles sur le marquage se doivent d'être claires et bien définies. Par exemple, il faut fixer des limites à la classification des renseignements confidentiels pour assurer le marquage adéquat de ces données. L'enjeu a aussi été examiné sous l'angle des appareils domestiques intelligents qui recueillent de l'information sans supervision pour la retransmettre à des entrepôts ou des entreprises.

Lacune : Marquage manuel des données. Cet enjeu a produit le moins de résultats, sans doute parce qu'il se rapporte le plus à des technologies émergentes comme l'IA, la reconnaissance faciale et les médias sociaux. La recherche a fait ressortir seulement 27 normes de niveau I ou II. Onze relèvent des mots clés « contrôle de la qualité des données » et couvrent les facteurs de gestion de la qualité en général, ce qui recoupe l'enjeu 47. Cependant, quelques normes semblent porter sur des éléments vitaux de l'enjeu, comme la classification des renseignements confidentiels (norme ISO/IEC 19790) et les solutions à base d'étiquettes pour les analyses des médias sociaux (norme ISO 19731). La norme intitulée *Technologies de l'information – Intelligence artificielle – Examen d'ensemble de la fiabilité en matière d'intelligence artificielle* (ISO/IEC TR 24028), publiée en mai 2020, encadre aussi la sélection et la création objectives de jeux de données pour la formation ou la mise à l'essai. En résumé, s'il existe des normes sur certains aspects de cet enjeu, d'autres manquent cependant au paysage normatif, dont certaines nouvelles technologies comme les appareils intelligents qui recueillent de grandes quantités d'information. Les nouveaux systèmes automatisés en sont encore à l'étape du prototype; l'être humain continue d'intervenir dans leur mise à l'essai. Toutefois, puisque certains algorithmes peuvent détecter et encoder de l'information plus précisément que l'être humain, quel rôle ce dernier doit-il jouer dans la détection des biais?

Besoins en recherche et développement? Non

Recommandation : Élaborer une norme générale sur le marquage des données pour les appareils connectés à l'Internet des objets. La reconnaissance faciale n'est qu'un exemple parmi d'autres.

Degré de priorité : Élevé

Organisation(s) : OEN accrédités par le CCN

Enjeu 16 – Gestion des métadonnées

Cet enjeu couvre la collecte, la nomenclature, la gestion, l'accessibilité et la viabilité des métadonnées. Sa portée est incertaine, les métadonnées étant recueillies et gérées dans toutes sortes de contextes, y compris dans le cadre de bases ou de jeux de données structurés et sur le Web. Il existe aussi différents types de métadonnées (descriptives, structurelles, statistiques, etc). On entend par « gestion des métadonnées » la conception, l'adoption et l'adaptation d'un schéma qui consiste en éléments ou attributs « méta » mettant en contexte la base ou le jeu de données ou toute autre ressource numérique.

17 New Work Item Proposal

Les données sont souvent le produit de divers procédés techniques. Tout comme l'évaluation de l'aptitude à l'emploi détermine la pertinence de ces données, la gestion des métadonnées détermine leur fiabilité. Les métadonnées servent à consigner l'utilité et la qualité des données à cette fin. Pour éviter les duplications, l'évaluation de la qualité devrait donc se concentrer sur les métadonnées plutôt que sur les données. Si les critères d'évaluation des unes et des autres ont beaucoup de points en commun, ils devraient différer en ce qui a trait à cet enjeu.

Les mesures de protection ont également été étudiées en lien avec l'accès à la collecte aux fins de gestion des données. Certaines métadonnées sont elles-mêmes confidentielles, indépendamment des données. Le regroupement des données a des répercussions sur la gestion des métadonnées, puisqu'il faut tenir compte des contrôles d'accès et des personnes autorisées à obtenir, modifier et consulter les données. Quant à la relation entre les mesures de protection et les métadonnées, ces dernières peuvent revêtir une grande valeur quand elles servent à des fins commerciales. Elles peuvent donc soulever des questions d'éthique, par exemple concernant la sécurité et les règles sur le partage. Toutefois, les protections de la LPRPDE peuvent alors s'appliquer.

L'analyse s'est ensuite penchée sur l'importance de la qualité des métadonnées et son lien avec le type de données. En marketing, par exemple, on pourrait tolérer une plus grande marge d'erreur que dans le domaine de l'équipement médical. Par conséquent, le même standard ne peut s'appliquer à toutes les données. Il faut clairement distinguer les données des métadonnées. Ces dernières sont souvent qualifiées de données sur les données, définition qui manque de clarté. L'idée de parcours des données, qui englobe tous les processus par lesquels elles passent, importe ici, car il y a différents types de métadonnées (techniques, scientifiques, etc.). D'autres définitions divisent les métadonnées en trois catégories : opérationnelles (pour la gouvernance des données); techniques (sur le parcours des données); et commerciales (sur le traitement et la consultation des données). De plus, la gestion des métadonnées est largement liée aux questions de visibilité, d'aptitude à l'emploi, de qualité et de collecte des données. Il est recommandé d'étudier les schémas de métadonnées en place – comme le jeu de métadonnées Dublin Core, le Profil d'application de métadonnées du gouvernement ouvert – dans la recherche et l'analyse des lacunes pour cet enjeu. La Norme sur les métadonnées du Conseil du Trésor contient d'autres exemples de normes pertinentes et largement adoptées sur le sujet.

Lacune : Gestion des métadonnées. Bien que cet enjeu couvre une vaste gamme de sujets qui ne sont pas tous clairement définis, la recherche de normes a produit des résultats intéressants. La plupart des éléments clés de l'enjeu, comme la collecte de métadonnées, la nomenclature, l'accès, la sécurité, la sémantique et les ontologies semblent couverts par des normes distinctes, surtout la collecte. Ce sont les normes ISO 23081-1 et 23081-2 qui semblent couvrir le plus de volets, dont la création, la capture, l'entretien et l'accès. Constituée de principes, la première, intitulée *Information et documentation – Processus de gestion des documents d'activité – Métadonnées pour les documents d'activité – Partie 1 : Principes* (ISO 23081-1:2017), fait le lien entre les exigences relatives aux métadonnées et les grands énoncés déontologiques de la norme de base ISO 15489-1. La deuxième, intitulée *Information et documentation – Gestion des métadonnées pour l'information et les documents – Partie 2 : Concepts et mise en œuvre* (ISO 23081-2:2009), adopte une approche pratique de la mise en œuvre. Elle traite des options de mise en œuvre, de la gestion des métadonnées et du modèle conceptuel à utiliser pour définir les éléments de métadonnées des documents. Deux bémols : premièrement, aucune norme générique ne semble exister sur les questions de sémantique et les systèmes de métadonnées. Il existe par contre des normes sectorielles pour ces deux sujets. Deuxièmement, aucune des normes ne mentionne le parcours des données, ce qui pourrait révéler un manque à combler du côté de l'exhaustivité des métadonnées sur les processus subis par les données.

Besoins en recherche et développement? Non

Recommandation : Élaborer une norme pour uniformiser les définitions et combler les lacunes concernant l'échange de données et la communication d'information aux utilisateurs.

Degré de priorité : Moyen

Organisation(s) : OEN nationaux, régionaux et internationaux

Enjeu 17 –
Politiques sur les données : gestion des risques et stratégies dans les organisations

Cet enjeu concerne la gestion des risques et les stratégies en matière de politiques sur les données, lesquelles peuvent varier d'une industrie à l'autre, ainsi que les risques d'incohérence, qui peuvent compliquer les choses. Les politiques sur les données peuvent se concentrer sur certains aspects et s'appuyer sur d'autres politiques comportant des exigences relatives aux renseignements. Les stratégies organisationnelles doivent tenir compte de nombreuses sources d'information, ce qui oblige chaque service et organisation à se doter de politiques sur l'intégration des données. Autres sujets à l'étude : la portabilité de l'information, c'est-à-dire le contrôle qu'exerce le propriétaire sur les données.

La gestion des risques associés à la confidentialité en ce qui touche le regroupement des données, l'évaluation des facteurs relatifs à la vie privée et les stratégies d'anonymisation a fait partie de l'analyse. Le cadre stratégique lui-même comporte d'ailleurs son lot de risques. À cet égard, la Charte canadienne du numérique semble constituer un excellent exemple de mécanisme de gestion, même s'il faudra des mécanismes pour assurer la conformité aux politiques. Enfin, il y a un lien clair entre cet enjeu et celui de la gouvernance en ce qui concerne l'accès et les contrôles.

Lacune : Politiques sur les données : gestion des risques et stratégies dans les organisations. La recherche a généré de nombreuses normes sur le sujet. Il en existe sur la gouvernance des données, la responsabilité, les règles, les politiques, la protection et la portabilité des données, qui peuvent s'appliquer à divers contextes : IA, infonuagique, secteurs précis ou différents types de données. Il y a lieu de les étudier pour déterminer si elles sont cohérentes, et s'il faudrait une norme plus générique ou si les normes en vigueur couvrent tous les aspects de l'enjeu. On ignore pour l'instant si ces normes traitent des mécanismes de conformité.

Besoins en recherche et développement? Non

Recommandation : Cet enjeu est étroitement lié aux délibérations du groupe de travail 1, notamment l'enjeu 14. Il faudrait élaborer une norme générique qui comprendrait des mécanismes de conformité, conformément aux recommandations du groupe de travail 1.

Degré de priorité : Faible

Organisation(s) : OEN nationaux, régionaux et internationaux

Enjeu 18 –
Qualité et aptitude à l'emploi des données

Cet enjeu concerne la production cohérente de rapports sur la qualité des données, notamment les métadonnées recueillies régulièrement pour assurer cette qualité. Celle-ci se définit de nombreuses façons, habituellement à l'aide de cinq à dix critères qui couvrent toujours les mêmes concepts : pertinence, cohérence, actualité, précision, exhaustivité, constance, accessibilité, objectivité, lisibilité, originalité, utilité, exactitude, interprétabilité, fiabilité, etc.

Il convient d'étudier les cadres nécessaires au processus d'évaluation de la qualité et les moyens de mesurer cette qualité. Des bonnes pratiques doivent être définies et adoptées pour assurer la mise en place de ces cadres. L'enjeu devrait comprendre un volet de responsabilisation et de répartition des pouvoirs. Il définit par ailleurs la qualité en fonction des résultats du profilage des données. Or, pour réduire les coûts, certaines organisations sautent l'étape du profilage. Cet élément du cycle de vie devrait pourtant être obligatoire, puisque sans lui, il est impossible de bien évaluer la qualité des données. Il faudrait déterminer quels sont les critères minimaux de qualité et comment les mesurer. La réponse dépendra beaucoup du type de données. La notion de temps interviendra aussi, puisque certains s'interrogent sur les effets sur la qualité et la pertinence des données du passage du temps depuis leur collecte. Ces questions s'inscrivent dans le concept d'actualité.

L'analyse s'est également penchée sur la qualité des données dans le contexte du cycle de vie, de la prise en charge, du traitement et de l'exportation. Dans les travaux actuellement menés pour concevoir un cadre fédéral sur la qualité, celle-ci a été liée à l'aptitude à l'emploi, certains aspects de la qualité étant « internes » (les caractéristiques mêmes des données), tandis que d'autres sont « externes » (l'utilisation faite des données). Une approche semblable, mais potentiellement déroutante, consiste à distinguer entre l'objectif et le subjectif. Comme on l'a dit, le concept de qualité est lié à celui de l'aptitude à l'emploi, c'est-à-dire qu'il dépend des besoins de l'utilisateur, mais son évaluation se fonde sur des mesures ou des indicateurs objectifs. Ces derniers peuvent être qualitatifs ou quantitatifs et doivent être définis avant l'évaluation. On compte parmi les critères à considérer la source de l'information (si elle est fiable et constitue une autorité sur le sujet). Étant donné la portée limitée de cette évaluation, l'accent doit rester sur la description des jeux de données et des méthodes employées pour compiler et recueillir l'information. Cette description doit être claire pour que l'utilisateur puisse déterminer l'aptitude à l'emploi des renseignements. Le but premier doit être la création de métadonnées sur les données, leurs attributs et les systèmes de cotation. Il faut utiliser avec prudence les systèmes de cotation, surtout s'ils produisent une note unique à la fin du processus, car les critères de qualité n'ont pas tous la même importance pour tout le monde. Enfin, l'enjeu se rapporte en partie à la gestion des métadonnées.

Lacune : Qualité et aptitude à l'emploi des données. Beaucoup des résultats générés par la recherche dans ce domaine renvoient à la norme ISO 8000 sur la qualité des données. Bien qu'elle ne s'applique pas nécessairement à tous les contextes, cette norme forme une bonne base pour la gestion de la qualité. D'autres normes visent des secteurs en particulier, et notamment les paramètres d'évaluation à utiliser. Chaque référence a ses propres critères et définitions. Faudrait-il composer une définition standard de la qualité? Si oui, il s'agit d'un manque à combler. Il existe par exemple une norme sur les données géographiques qui décrit explicitement l'importance des métadonnées dans l'évaluation de l'aptitude à l'emploi.

Besoins en recherche et développement? Non

Recommandation : Quoique la norme ISO 8000 offre un bon point de départ, elle ne suffit peut-être pas à tous les secteurs. Il faudrait créer une norme plus exhaustive, qui tient compte des aspects de fiabilité et de transparence dans l'évaluation de l'aptitude à l'emploi.

Degré de priorité : Moyen

Organisation(s) : OEN nationaux, régionaux ou internationaux.

Groupe de travail 3 : Accès, diffusion et conservation

Enjeu 19 – Gestion du consentement (autorisation, accès et retrait)

Cet enjeu englobe les aspects du consentement qui se rapportent à l'accès aux données. La gestion du consentement, c'est en quelque sorte un processus qui sert à rendre le système conforme à la réglementation sur la protection de la vie privée en obtenant la permission de l'utilisateur pour la collecte de données à son sujet. Bien que ce consentement soit obtenu à l'étape de la collecte, l'enjeu porte sur son rapport avec la consultation et l'utilisation des données en temps réel. La personne visée doit pouvoir vérifier qui s'occupe des consentements pour accéder à toutes les permissions qu'elle a signées; en effet, impossible de supprimer des données si on ne sait pas où elles se trouvent. Des mécanismes doivent être en place pour guider la personne et l'informer au sujet du consentement. Il faut poursuivre les discussions sur la précision du consentement pour déterminer la part de données visée par celui-ci. Il faut savoir que l'identité ne se limite pas à la personne, mais comprend aussi ses identifiants uniques. Les éléments suivants ont été exclus de l'analyse pour cet enjeu :

- Gestion du consentement des entités, dont il sera question dans une autre section;
- Méthode de stockage des données dans le contexte des dossiers électroniques sur la santé, des fiducies de données, du stockage en ligne personnel, etc.;
- Principes généraux (hébergement, utilité, destinataire, précision, etc.) qui pourraient faire l'objet de nouvelles normes;
- Suivi des changements aux données stockées et du consentement correspondant.

Le consentement se compose de nombreuses facettes qui compliquent la définition des mécanismes régissant la façon dont une personne donne ses renseignements. Puisque les perspectives varient sur les moyens d'accéder aux données, il faudrait adopter un langage commun pour simplifier les discussions entre les autorités de réglementation, les innovateurs et les consommateurs. Beaucoup de définitions ont été proposées et publiées, mais elles ne font pas l'unanimité, et l'adoption des termes définis porte encore à confusion. Une description de l'accès aux données servirait à définir qui donne l'accès et à quoi, étant donné que le consentement passe par diverses plateformes. De plus, le concept de consentement amène à se demander s'il s'agit d'un renoncement contractuel à des renseignements personnels. Seules les personnes concernées sont responsables de consentir aux divers services qu'elles retiennent; elles ont donc besoin d'un outil définissant la nature du consentement donné. L'élaboration d'une norme sur le transfert du consentement serait alors la solution idéale. Le consentement doit être éclairé, et la personne qui le donne doit être informée de l'utilisation visée. Sinon, elle ne sait pas à quoi elle consent.

Il faudrait mettre en place des mécanismes pour que les gens se sentent à l'aise de donner leur consentement sans passer les conditions au peigne fin. Le public doit pouvoir faire confiance au système et croire à l'existence intrinsèque de mécanismes de surveillance et d'intendance. Ce concept est difficile à définir et codifier, mais les normes sur ces mécanismes sont très importantes. La définition de la confiance dans le contexte du consentement est une avenue à explorer dans la normalisation pour combler les lacunes de cet enjeu. Le Cadre de confiance pancanadien emploie des ensembles de règles et d'outils conçus pour inspirer confiance dans le système, mais rien n'a été créé pour assurer aux particuliers que l'entité à qui ils confient leurs données les utilisera correctement. Les normes pourraient aborder les moyens d'améliorer l'utilisation des données et définir les cas où il est permis d'utiliser des données à des fins non consenties, avec les niveaux de regroupement et d'assurance associés.

Lacune : Gestion du consentement (autorisation, accès et retrait). Selon les sept principes directeurs pour le consentement valable du Commissariat à la protection de la vie privée du Canada, la personne doit pouvoir comprendre la nature, le but et les conséquences de son consentement. Pour que le consentement soit valable ou approprié, l'organisation doit expliquer à la personne, en termes exhaustifs et compréhensibles, ses pratiques en matière de protection de la vie privée.

Selon l'analyse, cet enjeu a généré un grand nombre de normes sur le consentement à la collecte, l'accès aux données et le consentement au retrait de données. Ces normes portent sur des sujets essentiels à l'enjeu et ont été mises à jour en fonction des nouvelles pratiques de collecte. Étant donnée la récente montée en valeur commerciale des données, la collecte et le stockage de grandes quantités d'information ont rendu nécessaire la tenue de nouvelles activités de normalisation visant le traitement des cas de non-conformité et des erreurs dans le processus de validation du consentement.

L'évolution des technologies vient altérer le traitement légitime des renseignements personnels. Voilà pourquoi il faut des normes concises sur la gestion du consentement. Les normes étudiées dans l'analyse ne traitent pas des consentements entre machines ni des mécanismes qui encadrent l'accord du consentement tout au long du processus, autant de domaines où il faudrait plus de recherches. En autres volets problématiques de la gestion du consentement, on compte la classification des données anonymisées et l'identité numérique.

Besoins en recherche et développement? Oui (classification des données anonymisées, utilisations primaires et secondaires des données, nécessité de l'identification du destinataire)

Recommandation : Élaborer un cadre indépendant de vérification pour la gouvernance des données, comme il en existe pour la comptabilité, afin de favoriser la conformité. Pousser la recherche pour déterminer comment l'identité numérique peut contribuer à la gestion du consentement et comment le consentement est accordé pour les données anonymisées (manque de classification pour ce type d'information).

Degré de priorité : Élevé

Organisation(s) : Conseil d'identification et d'authentification numériques du Canada (CCIAN), Consortium World Wide Web (W3C), Commissariat à la protection de la vie privée du Canada

Enjeu 20 – Accès aux données

D'ici 2021, il y aura près de 4,5 milliards d'utilisateurs Internet dans le monde générant plus de 3 zettaoctets de données. Dans ces conditions, comment trouver le bon entrepôt de données et y accéder sans risque? C'est la question à laquelle pourraient répondre les normes. Trouver les données, voilà le problème. Il faudra pour cela uniformiser les contrôles d'accès fondés sur les rôles ou les métadonnées utilisées pour classer les données par degré de confidentialité (et ainsi en réglementer l'accès).

Cet enjeu est récurrent pour le groupe de travail 3 et couvre plusieurs aspects du processus d'autorisation d'accès aux données. Comment peut-on mieux définir l'accès dans le cadre de cet enjeu pour mieux l'encadrer? C'est aussi une question d'accès sémantique.

Sujets inclus dans l'enjeu :

- Types d'accès (aléatoire ou séquentiel);
- Procédure d'accès (marche à suivre pour accéder aux données) – Avant même d'accéder aux données, il faut savoir si elles seront utiles à l'analyse. L'enjeu 27 porte sur l'accès aux métadonnées, un autre aspect clé de cet enjeu;
- Interrogation et recherche de données;
- Convivialité et clarté de la marche à suivre pour accéder aux données (il ne devrait pas être nécessaire d'être un expert) – Les métadonnées peuvent faciliter ce processus en faisant ressortir les permissions nécessaires. Il pourrait y avoir une norme sur les demandes d'accès aux métadonnées ainsi que des principes sur l'accès aux données (étape par étape);

- Premier élément – Définition du jeu de données (interrogation, langage SQL, etc.);
- Deuxième élément – Contrat entre le consommateur et le fournisseur de données sur l'extraction du jeu de données, le but, la valeur temporelle, etc.
- Troisième élément – Contrôles. Une fois la permission accordée, où doit-on aller pour prendre contrôle des chaînes de connexion (supprimer des connexions, modifier des permissions, etc.)? Possibilité de révoquer un accès;
- Accès aux jeux de données à des fins d'analyse exploratoire (explication et contrat concernant la manière d'accéder aux jeux de données);
- But de l'accès (l'utilisateur a l'obligation de préciser à quoi serviront les données);
- Restrictions et politiques – Quels types de normes les fournisseurs peuvent-ils utiliser pour restreindre les jeux de données fournis (destruction après utilisation initiale, interdiction d'envoyer les données à un tiers, valeurs temporelles)?

Sujets non inclus dans l'enjeu :

- Découverte des données (l'accès aux données est principalement une question de permission, de sécurité et de rôles.) – Certains éléments font partie d'autres sections (l'enjeu 52 sur le marquage et la traçabilité des données), mais la question de la visibilité n'a pas été retenue.

La liste des renseignements existants doit être consignée et facilement accessible (ex. : dans Google ou un autre moteur de recherche) pour qu'on puisse ensuite trouver ces renseignements. Cela facilite la recherche uniforme de sources pertinentes. Aujourd'hui, il est difficile de savoir où trouver des données de qualité. Par exemple, afin de garantir le droit d'accès à l'information, une loi a été adoptée pour créer un outil de publication qui normalise la manière dont les établissements gouvernementaux présentent leurs sources. C'est une stratégie essentielle à l'application des droits d'accès à l'information et à leur intégration dans la *Loi sur l'accès à l'information*. Les descriptions doivent être standardisées, c'est-à-dire qu'elles doivent comprendre les mêmes éléments. Voir les enjeux de visibilité et d'accès aux métadonnées du groupe de travail 2.

Il y a un manque de normes sur l'attribution des droits d'accès aux données, et de cadre qui indiquerait quel processus utiliser. De plus, cet enjeu implique la nécessité de pouvoir retrouver ses renseignements personnels pour les supprimer. Entre autres sujets sur lesquels les normes pourraient se prononcer, on compte :

- la convivialité et la transparence du processus d'accès aux données, bien que les normes à ce sujet se trouvent plutôt dans l'enjeu sur la visibilité des données (groupe de travail 2);
- l'obligation pour le consommateur, s'il veut accéder à un jeu de données, d'en faire la demande. L'ambiguïté réside dans la définition des données et de la période d'accès, d'où l'utilité d'une norme sur le sujet (pour l'interrogation et le contrat, qui fixe les paramètres que doit respecter le consommateur);
- la restriction de l'accès aux données par le consommateur selon les besoins, les fins visées et les demandes.

Lacune : Accès aux données. Selon l'analyse, un grand nombre des normes générées par la recherche se sont avérées non pertinentes. La plupart des normes pertinentes semblent assez générales, et traitent de sujets tels que les contrôles d'accès et la protection de la vie privée au moyen de chaînes de blocs. Cependant, ces normes ne touchent pas aux contrôles d'accès dans le contexte des mégadonnées, de l'intelligence artificielle et de l'apprentissage machine.

Les mégadonnées compliquent l'échange de données; il sera important de mener des recherches et d'élaborer de nouvelles normes pour combler cette lacune et améliorer l'accès à l'information.

Besoins en recherche et développement? Oui. Il faut adapter les contrôles d'accès aux mégadonnées, aux liaisons de données et à la gestion des permissions.

Recommandation : Créer un mécanisme de vérification pour assurer la conformité.

Degré de priorité : Moyen

Organisation(s) : ISO/IEC, British Standards Institution

Enjeu 21 – Conservation des données

Cet enjeu concerne les normes qui doivent être créées pour établir, au sein d'une organisation, une procédure de conservation des données autres que les renseignements personnels. Une approche rigoureuse à cet égard préciserait combien de temps les données doivent être conservées et comment s'appliquent les exceptions en cas de poursuite ou d'autres interruptions. La procédure devrait aussi traiter des éléments suivants :

- Période de stockage et communication de renseignements à ce sujet
- Raison ou besoin opérationnel justifiant la conservation des données (équilibre entre la protection de la vie privée et les avantages économiques)
- Motifs et méthodes de collecte des données
- Possibilité d'accepter ou de refuser la divulgation des renseignements
- Organisation des données à des fins futures
- Élimination des données devenues inutiles
- Droit à l'oubli

Le calendrier de conservation à adopter peut dépendre du secteur et des règlements qui le régissent. C'est alors que les cas d'utilisation prennent tout leur sens. En général, on recommande l'inclusion, dans les politiques, d'un plan de conservation des données établissant une date ou un événement précis (ex. : 30 jours après un webinaire) et la mesure à prendre (suppression de toutes les données sur un sujet donné). La gestion du cycle de vie sert à évaluer la quantité de données détenues et à en faire quelque chose d'utile pour plus tard, dans un format différent de l'original. Des spécifications devraient être en place pour le stockage sécuritaire des données, ainsi qu'un processus pour l'archivage dans un autre format. Les normes sur la protection des données qui s'appliquent aux données actives devraient également s'appliquer à ces données conservées.

La classification des données est un élément capital de cet enjeu. La nature des renseignements – personnels, essentiels, primaires ou publics – joue un rôle dans la façon dont ils sont traités selon la politique de conservation. De plus, les entités doivent assurer la conservation, non seulement des données, mais aussi de leur structure. Le calendrier de conservation doit donc tenir compte de la possibilité ou non de retirer quelque chose de la base de données sans en défaire la structure. Il convient de souligner que les formats et médias exclusifs pourraient compliquer l'utilisation des données d'ici 10 à 15 ans, parce que la technologie évolue. Le commissaire à la protection de la vie privée doit éviter que la structure des données serve d'excuse à leur non-suppression. Les politiques de la fonction publique de l'Ontario abordent le sujet, surtout pour les systèmes vieillissants. Elles permettent de relier la conservation des données à la mise hors service du système, plutôt qu'à un événement ou à une date en particulier.

Il y a lieu de définir comment les règlements s'appliqueront à la conservation des données et quels types de pratiques peuvent encadrer la conservation à long terme. Si la commercialisation des données donne lieu à des modèles d'affaires avantageux, il faut un processus décisionnel éclairé pour déterminer combien de temps conserver des renseignements personnels après leur collecte ainsi que quand et comment les supprimer. La conservation des données comporte un volet temporel, seulement pour les courtes périodes. La durée de conservation peut varier d'un secteur à l'autre – à voir au cas par cas. D'autres domaines nécessitent de plus amples recherches sur les pratiques exemplaires : le droit à l'oubli et les systèmes bancaires ouverts (où le fournisseur doit demander la permission du client, qui reste propriétaire des données).

Les règlements sur la conservation pourraient servir à encadrer certains aspects particuliers de la protection des données, mais les normes sur cette dernière devraient constituer une catégorie en soi. Les experts en gouvernance des données travaillent sur la question depuis un certain temps; l'accent devrait donc être mis sur l'accroissement net du volume de données, comme dans le cas de l'ajout de grandes quantités de données recueillies par les appareils de l'Internet des objets avant d'être regroupées et utilisées, parallèlement à la perte de beaucoup des données originales. Les transferts, les échanges et la portabilité font partie de l'enjeu.

Lacune : Conservation des données. La recherche sur cet enjeu a généré des normes de qualité sur des sujets comme le droit à l'oubli, les limites de stockage et l'élimination, la gestion des enregistrements et l'archivage des données (aspects clés de la conservation). On peut en conclure que la question a attiré l'attention des réseaux de normalisation et des autorités de réglementation, qui ont alors conçu des pratiques exemplaires.

La recherche a révélé l'existence de documents d'orientation sur les questions entourant la collecte de données par des organisations qui comptent les utiliser à d'autres fins que celles énoncées au départ. Peu de règlements régissent la durée de conservation des nouvelles données par les intendants. Il n'y a pas non plus de norme unique sur les entités hébergeant ces nouvelles données.

Pour terminer, la recherche initiale n'a révélé aucune lacune à cet égard, mais il pourrait être nécessaire de pousser l'analyse pour le confirmer, notamment en ce qui touche aux pouvoirs des intendants.

Besoins en recherche et développement? Normes sectorielles sur la conservation des données (chaque secteur a ses propres règlements, par exemple les banques conservent leurs données pendant 7 à 10 ans).

Recommandation : Créer un cadre ou un mécanisme de vérification de la conformité.

Degré de priorité : Moyen/Faible

Organisation(s) : Commissariat à la protection de la vie privée du Canada

Enjeu 22 – Gestion de l'identité : validation et authentification des individus, entités et appareils

Cet enjeu englobe la terminologie et les concepts propres à la gestion de l'identité, pour la promotion d'une définition commune. Il couvre la gestion et l'authentification des identités individuelles, de même que les autorisations, les rôles et les privilèges qui s'y rapportent, sans égard aux démarcations.

Les consommateurs ont maintenant l'habitude de se créer des comptes auprès de différents fournisseurs pour accéder à leurs services. Dans ces cas, tous les attributs de l'identité doivent être vérifiés pour assurer le fonctionnement du système et éviter les pertes de données. La gestion de l'identité s'inscrit alors dans un ensemble de politiques et de technologies servant à vérifier que les bonnes personnes ont accès aux bonnes ressources technologiques.

Or, le cadre de gouvernance actuel manque de normes sur les identifiants numériques utilisés pour l'identification personnelle. L'identité numérique vient corriger certains manquements de la gestion de l'identité en facilitant l'évaluation et l'authentification de l'information au moyen d'un système commercial en ligne, sans intervention humaine. Parmi les domaines à normaliser davantage, on compte aussi les identifiants cryptographiques et les réseaux d'identités.

Lacune : Gestion de l'identité : validation et authentification. Pour être rigoureux, le modèle de gouvernance des données doit être doté d'un système de gestion de l'identité. Ce dernier offre une protection supplémentaire en assurant l'application cohérente des règles et politiques d'accès à l'échelle de l'organisation.

Selon l'analyse, la plupart des normes générées par la recherche pour cet enjeu se rapportent bien à la gestion de l'identité et à ses attributs. Elles couvrent divers sujets tels que les identifiants cryptographiques, l'authentification multifacteur, les données biométriques, les portefeuilles numériques et l'identité. Les méthodes d'authentification devront évoluer au même rythme que la technologie pour rester pertinentes. Il faudra peut-être poursuivre les recherches pour savoir si des technologies émergentes comme l'IA et l'apprentissage machine améliorent ou compliquent les méthodes de validation et d'authentification. Certaines sources laissent entendre que ces technologies assument maintenant les fonctions exécutives de l'identité et de l'accès, domaines où l'on recourt à des interventions fluides plutôt qu'aux pare-feu pour contrer les menaces. Ce pourrait être autant de sujets présentés au CCIAN dans l'application du Cadre de confiance pancanadien.

Besoins en recherche et développement? Oui, sur les effets de l'intelligence artificielle et de l'apprentissage machine sur la gestion de l'identité, et sur l'effet facilitant ou non de ces technologies sur les méthodes de validation et d'authentification.

Recommandation : Consulter le CCIAN au sujet de la gestion de l'identité.

Degré de priorité : Élevé

Organisation(s) : OEN accrédités par le CCN, CCIAN, Centre canadien pour la cybersécurité

Enjeu 23 – Partage, échange et intégration des données

Cet enjeu couvre les principes directeurs du partage, de l'échange et de l'intégration des données. Il faut préciser que chacun des sujets abordés comporte un volet de confidentialité dont il faut tenir compte dans le modèle de gouvernance des données. La mise en relation de différentes sources d'information fait partie intégrante de l'enjeu, tout comme les éléments suivants :

- Méthodes techniques d'échange des données
- Méthodes de chiffrage
- Terminologie normalisée pour les ententes de partage des données
- Processus d'évaluation des conséquences du partage

L'échange se fait dans le cadre d'une entente bilatérale entre deux parties, élément central du concept. Est à définir la manière dont seront régies les activités de partage, d'échange ou d'intégration des données selon l'endroit. L'enjeu concerne principalement les résultats de la décision d'intégrer divers jeux de données, avec ou sans consentement. À noter qu'il faut aussi porter attention aux biais pour s'assurer les bons résultats, et que ces derniers pourraient nécessiter une plus grande transparence.

Le partage de données, c'est la capacité pour plusieurs applications ou plusieurs utilisateurs de partager les mêmes ressources sans les changer. Plus général, l'échange est multilatéral et touche un éventail de consommateurs et de fournisseurs de services. L'entente est implicite au partage. On peut donc se demander, une fois l'information partagée, comment savoir si elle sera utilisée de nouveau ou comment assurer la transparence de cette utilisation.

L'intégration des données, c'est leur interprétation par le destinataire. Il faut comprendre la relation entre les parties quand il s'agit d'intégrer différentes sources d'information.

Les facteurs inconnus qui interviennent dans le processus de partage, d'échange et d'intégration détermineront quelles politiques doivent être employées. Par exemple, le partage ne crée pas de copie, contrairement à l'échange. Ce qui se passe après coup ne peut être géré ou contrôlé. On ignore quels sont les risques associés au stockage de données échangées dans une mémoire cache, comme c'est le cas pour les données de patients utilisées à des fins autres que celles énoncées lors de la collecte.

Lacune : Partage, échange et intégration des données. Plus la valeur des données augmente, plus les ententes ou contrats de partage, d'échange et d'intégration des données se compliquent. Dans un milieu aussi effervescent, les intendants des données trouvent difficile de gérer la collaboration entre les clients. L'analyse l'atteste : la plupart des normes étudiées pour cet enjeu se sont avérées non pertinentes ou propres à un secteur (transmission de signaux pour les services publics, télécommunications et transport). Il faudrait uniformiser la terminologie des ententes ou des cadres de partage des données, en portant attention au contrat lui-même, qui pourrait inclure un processus d'évaluation des conséquences du partage pour combler les lacunes pour cet enjeu. Par exemple, le cadre sécurisé de partage de données de Singapour définit trois modèles généraux de partage (bilatéral, multilatéral et décentralisé) pour guider le processus. Ce qu'il reste à préciser, c'est la normalisation des aspects contractuels, et non le langage technique.

Besoins en recherche et développement? Oui. Il est nécessaire de pousser la recherche afin de déterminer quels domaines clés prioriser pour jeter les bases de la collaboration. Il y a également lieu de normaliser les aspects contractuels du partage des données plutôt que le langage technique.

Recommandation : Concevoir des mécanismes pour assurer la conformité.

Degré de priorité : Moyen

Organisation(s) : OEN accrédités par le CCN, Contracts for Data Collaboration (C4DC)

Enjeu 24 – Fiabilité des intermédiaires du traitement des données

Cet enjeu porte sur les façons dont les intermédiaires assurent l'intendance fiduciaire indépendante des données. L'analyse servira à cerner comment l'intermédiaire régit l'information et quelles sont les conséquences d'un retrait de données ou d'autorisation d'utilisation. Il manque de normes applicables aux intermédiaires fiduciaires qui se concentreraient sur ces derniers plutôt que sur les répertoires de données. Serait-il possible, dans un cadre de gouvernance, d'instaurer une fiducie pour gérer uniquement l'aspect de l'accès? Il est essentiel de concevoir des normes régissant les entités qui stockent les données partagées de plusieurs parties, pour en garantir l'indépendance et l'équité.

Par définition, l'intermédiaire est un courtier en information, mais sa fonction première doit être étudiée plus en détail. Sa nature même lui donne un rôle minimaliste, même s'il y a des cas où il doit assumer d'autres fonctions. Il joue plusieurs rôles selon l'étape du cycle de vie des données, d'où l'utilité de définir ces rôles. Pour qu'un intermédiaire agisse en fiducie, il doit adhérer à plusieurs normes pour démontrer certaines qualités, preuves de sa conformité. Une certaine forme de vérification doit faire l'objet d'une normalisation (vérification de l'intermédiaire, en cas de non-conformité à une entente de niveau de service). Quels sont les éléments qui confirment la fiabilité d'un intermédiaire fiduciaire? Ce ne sont pas toutes les organisations qui peuvent se dire fiables; elles doivent adhérer à certaines normes de cybersécurité et autres mesures de conformité, comme PayPal, qui table sur le manque de confiance entre le commerçant et son client. La fiabilité numérique ne fait cependant pas partie des responsabilités de l'intermédiaire. Toutes les entités doivent être identifiables.

Les normes utilisées dans le domaine de la santé, y compris les contrats numériques, facilitent le traçage des opérations de courtage, et le sujet ou le propriétaire des données y est vu comme un facteur dans la rédaction des politiques sur les données. Les normes peuvent donner aux intermédiaires le pouvoir de faire appliquer les règles sur le traitement des données et fixer des seuils minimaux à respecter pour s'assurer le statut d'intermédiaire fiable. Cet enjeu porte principalement sur la création et le partage des données. Les fiducies de données ont pour but d'encadrer la gestion des données et la prise de décisions à leur sujet; elles se forment quand une partie en autorise une autre à prendre des décisions sur des renseignements en son nom, dans l'intérêt d'un plus grand groupe d'intervenants. La notion d'intermédiaire fiduciaire appelle à la création d'un lien de confiance. Les principes de gouvernance de ces intermédiaires doivent être définis et des normes précises doivent être adoptées à leur égard. L'enjeu englobe aussi la séparation des données et des applications, ainsi que les répercussions du retrait de données ou de l'autorisation d'utilisation.

Lacune : Fiabilité des intermédiaires du traitement des données. Au Canada, le concept d'intermédiaire fiable du traitement des données n'est pas clairement défini. C'est l'occasion parfaite de créer des normes pour corriger ce manque et faire une distinction nette entre l'intermédiaire et le courtier en information. Qui plus est, les ententes entre l'intermédiaire et son organisation partenaire nécessitent l'établissement de paramètres mieux définis (ex. : droits de propriété sur les données, à court ou à long terme). Il incombe aux intermédiaires fiables d'étudier comment gérer leurs données au moyen d'un processus d'accréditation ou d'attestation visant à établir des principes fiables, un processus d'évaluation des demandes d'accréditation, et des pratiques fixes.

Selon l'analyse, très peu des normes générées par la recherche se sont avérées pertinentes. La plupart de celles qui l'étaient semblent porter sur l'obtention de données et de métadonnées plutôt que sur les facteurs de qualification, d'attestation et d'accréditation des intermédiaires fiables, le rôle et l'autorité de l'intendant des données, ou le cycle de vie des données et métadonnées. Il vaut la peine de noter que les normes jugées pertinentes ont été publiées récemment et que dans l'écosystème de normalisation, surtout en Europe, les lacunes à ce sujet ont été remarquées. Parmi les thèmes d'intérêt, on compte les syndicats de l'information, une solution hybride entre le courtier et l'intermédiaire.

Besoins en recherche et développement? On note un manque d'information sur l'accréditation et l'attestation des intermédiaires fiables. Comment ces derniers s'entendent-ils avec d'autres acteurs en ce qui concerne les droits, les autorisations d'accès et les licences?

Recommandation : Renommer l'enjeu « Fiabilité des intermédiaires du traitement des données ». Définir ce qui constitue un intermédiaire fiable au Canada. Préciser comment les intermédiaires s'entendent avec d'autres acteurs du milieu.

Degré de priorité : Moyen

Organisation(s) : OEN accrédités par le CCN

Enjeu 25 – Autorisation à la collecte et au partage de données

Cet enjeu concerne des aspects de l'autorisation, à savoir qui peut accéder à quels renseignements personnels, industriels ou commerciaux et quelles politiques sur les données sont en place pour protéger les renseignements confidentiels. Les mêmes critères de consentement (autorisation) ne s'appliquent pas aux renseignements industriels et aux renseignements personnels, ce qui explique la nécessité de créer un modèle de gouvernance segmenté. En effet, il serait difficile d'appliquer aux données industrielles et au traitement de l'information entre machines (ou systèmes) le même genre de contrat qu'aux données commerciales ou personnelles. Le contrat pourrait être partiellement intégré au logiciel ou régi par un contrat externe. Une interface de programmation d'applications (API) pourrait faciliter la création de paramètres d'autorisation clairs et l'accès restreint à certains dossiers.

Il serait nécessaire de déterminer qui peut contrôler la collecte et le partage des données, surtout dans les domaines industriel et commercial. Les organisations qui recueillent des données ont tendance à soutirer leur consentement aux gens sans protéger leur vie privée. De même, les données industrielles sont recueillies au moyen de contrats, mais les rapports de force ne sont pas toujours équilibrés (les petites entreprises n'ont pas les mêmes ressources que les grandes pour conclure des contrats de manière à pouvoir tirer parti des données). Or, consentir à l'utilisation d'un produit ou d'un service, c'est conclure un contrat.

La création d'un cadre normatif pourrait compliquer l'obtention d'autorisations lors de la collecte passive de données par les appareils de l'Internet des objets à des fins publiques et privées, puisque les données recueillies pourraient se retrouver dans les mains de plusieurs entreprises ou autorités. De plus, il faut attribuer à une instance la tâche de superviser et d'autoriser la collecte et le partage.

Autres aspects de l'enjeu à considérer : les appareils de collecte passive de données et leur utilisation commerciale (ex. : l'utilisation d'un drone pour prendre des photos du nombre de voitures, de piscines, etc. dans un quartier).

Lacune : Autorisation à la collecte et au partage de données (titre proposé : Autorisation à la collecte passive, à l'utilisation et au partage de données). Selon l'analyse, la plupart des normes générées par la recherche sur le sujet ont été jugées pertinentes. Elles portent entre autres sur la protection de la vie privée des utilisateurs pour les produits de l'Internet des objets et les lignes directrices sur le partage des données extraites des systèmes connectés et intelligents.

Cependant, à l'ère de l'économie des données, de plus en plus d'individus et d'entités tierces et indépendantes commencent à voir les possibilités et le potentiel commercial que présentent les données et à sortir des sentiers battus pour en trouver. Par exemple, les photos prises par un drone survolant un quartier peuvent être commercialisées et vendues au bon consommateur. Ce type de pratiques nécessite une autorisation (délivrée par une autorité) avec des paramètres pour encadrer le tout et protéger le droit à la vie privée des gens lors de la collecte passive d'information. En général, c'est dans ce domaine qu'il manque de normes.

Besoins en recherche et développement? Oui, sur les aspects légaux de l'enjeu

Recommandation : Renommer l'enjeu « Autorisation à la collecte passive, à l'utilisation et au partage de données », puisqu'il ne porte pas sur l'autorisation en général.

Degré de priorité : Élevé/Moyen

Organisation(s) : ISO/IEC

Enjeu 26 – Chiffrage

Cet enjeu devrait entre autres comprendre la méthode de chiffrage et ce qui est permis par un secteur ou des normes sectorielles. Le chiffrage est l'un des moyens de protéger des données partagées ou consultées, mais ce n'est pas le seul. De nouvelles solutions de protection et de confidentialité commencent à faire leur apparition, y compris pour les données synthétiques. Le chiffrage compte trois volets : les données inactives (dans les répertoires); les données en transit (envoyées à une autre partie); et les données remises au consommateur. Anciennement, il était difficile de protéger les données aux dernières étapes du cycle de chiffrage, jusqu'à ce qu'une nouvelle méthode, appelée « chiffrement homomorphique », permette de protéger les données même après leur remise au consommateur. Cette nouvelle technique permet au consommateur de consulter les données sans lui révéler certains détails sur le contenu du jeu de données.

Il faudrait normaliser les critères qui définissent ce qui est acceptable en matière de protection de la vie privée dans des contextes donnés. De plus, le manque de normes sur les limites d'utilisation des données par le consommateur soulève des questions. Que se passe-t-il du côté du consommateur? Comment les normes pourraient-elles multiplier les possibilités d'utilisation tout en respectant les règles de confidentialité et de protection de la vie privée? La mise en place de ces mécanismes sert à lever et atténuer les inquiétudes associées à l'utilisation des données. La gestion du chiffrage au fil du temps comporte son propre lot de difficultés, car ce qui est chiffré aujourd'hui pourrait être déchiffré demain. Les normes ne peuvent pas non plus prédire l'arrivée de nouvelles technologies. Selon certains chercheurs, par exemple, un ordinateur quantique serait capable de déchiffrer n'importe quel jeu de données.

Du point de vue du consommateur, la distinction entre les renseignements personnels et publics manque de clarté. Les groupes de travail 1 et 3 se sont penchés sur les aspects de protection de la vie privée, d'utilisation éthique des données et de cybersécurité de cet enjeu. Quant à l'anonymisation, en soi ou dans le contexte de cet enjeu, c'est un sujet qui a été traité séparément à l'enjeu 46. L'enjeu 49 sur les adresses IP devrait être confié au groupe de travail 4.

À noter la différence entre le chiffrage des données inactives, celui des données en transit et celui des données à l'étape de l'analyse.

Lacune : Chiffrage. Selon l'analyse, la plupart des normes générées par la recherche ont été jugées pertinentes. On voit, dans le milieu des normes, que plusieurs lignes directrices ont été adoptées sur le chiffrage homomorphique, ce qui révèle l'importance qui lui est accordée. D'autres efforts de normalisation pourraient se concentrer sur la définition de critères pour la protection de la vie privée dans des contextes précis, comme ceux de la confidentialité différentielle et des renseignements personnels ou publics.

Besoins en recherche et développement? Oui, sur la différence entre les renseignements personnels (non identifiables) et publics ainsi que sur la nécessité de préserver l'anonymat lors de l'acquisition des données.

Recommandation : Il se peut que cet enjeu soit en fait une question de réglementation ou de conformité plutôt qu'une question de norme. Une distinction pourrait être faite entre les renseignements personnels et publics avant le chiffrage. Des outils pourraient aussi faciliter la conformité.

Degré de priorité : Faible

Organisation(s) : ISO/IEC

Enjeu 27 – Gestion des ontologies

Dans cet enjeu, on verra la nécessité d'établir les principes (un langage intermédiaire) qui guideront l'utilisation de termes partageables et réutilisables sur l'interopérabilité des données stockées dans des bases. L'enjeu couvre la gestion des ontologies (vocabulaire, concepts et outils), en lien avec la gestion améliorée des données. Le but : assurer une compréhension commune de l'information, et ainsi la connectivité et l'interopérabilité des données, tout en augmentant leur valeur en facilitant l'interrogation et la consultation. Le processus de normalisation pourra se pencher sur la manière de définir les ontologies au Canada et mener à la création d'un registre canadien des ontologies assorti de normes de gouvernance. Les modèles ontologiques sont généralement exclusifs, d'où la nécessité d'établir un vocabulaire ouvert plutôt que contrôlé.

D'ailleurs, on manque de mécanismes en gestion des vocabulaires contrôlés; les concepteurs d'applications informatiques du domaine de la santé doivent disposer du vocabulaire médical normalisé correspondant, et c'est à leur avantage d'utiliser celui des normes en vigueur. Pour que ce soit possible, cependant, ces normes doivent répondre aux besoins des utilisateurs prévus. Dans les dix dernières années, les chercheurs en informatique médicale ont commencé à cerner certains de ces besoins, notamment en ce qui touche le contenu terminologique; l'orientation, la permanence et les identifiants non sémantiques des concepts; la polyhiérarchie; les définitions officielles; l'abandon des termes « non classés ailleurs »; les différents degrés de précision; la cohérence des différentes optiques; la représentation du contexte; l'évolution progressive et la redondance avérée.

Il est important de bien gérer l'ensemble des vocabulaires et ontologies (traduction d'une ontologie à l'autre) qui servent à l'interprétation sémantique des données rendues accessibles et des façons dont elles ont été chiffrées. Par exemple, quand quelqu'un accède à des données, il accède à de l'information chiffrée à la source, mais s'il n'a pas accès à l'ontologie, il ne pourra pas interpréter ces données. Les ontologies contribuent à la qualité des données et à leur compréhension. Par exemple, les systèmes de l'industrie pharmaceutique (Shoppers et Rexall) n'utilisent peut-être pas tous les mêmes termes pour traiter des mêmes médicaments. Pour que le traitement soit uniforme, il faut un vocabulaire uniforme. L'organisme Logical Observation Identifiers Names and Codes (LOINC) sert actuellement de référence terminologique commune pour les constats cliniques et laboratoires. Un système de référence semblable pourrait être créé pour d'autres secteurs.

Lacune : Gestion des ontologies (titre proposé : Terminologie de référence). La recherche de normes à ce sujet a donné des résultats neutres en matière de pertinence. La moitié des normes sont de niveau II (partiellement pertinentes), et l'autre moitié, de niveau III (propres à un secteur). Des vérifications supplémentaires ont révélé un manque à combler : il faudra mener plus de recherches afin de déterminer quels secteurs pourraient utiliser un « langage intermédiaire » pour l'échange de données interopérables.

Besoins en recherche et développement? Oui, sur les éléments de référence principaux et les systèmes de gestion des données de référence (LOINC).

Recommandation : Renommer l'enjeu « Terminologie de référence » et créer un outil pour encadrer les organismes qui produisent des ontologies.

Degré de priorité : Moyen

Organisation(s) : LOINC, National Center for Biotechnology Information

Enjeu 28 – Transparence, parcours et traçabilité des données

Cet enjeu concerne la transparence, le parcours et la traçabilité des données. Plus la législation se penche sur le cycle de vie des données, plus ces concepts gagnent en importance dans la gouvernance et la gestion de l'information. L'analyse a permis d'étudier la question dans l'optique des flux de données, de leur suivi et de leur facilité d'accès.

Par définition, le parcours des données désigne le trajet que suit l'information entre son point d'origine et son utilisation, tandis que la traçabilité désigne la possibilité de suivre en temps réel les activités et les flux de données qui les relient. S'ils ont le choix, les utilisateurs et propriétaires de données emploient une piste de vérification complète pour suivre l'utilisation qui a été faite de leurs données, tout en vérifiant et maintenant leur confidentialité. Une piste de vérification ne devrait pas révéler sur quoi portent les données, mais plutôt servir à l'élaboration des droits à la confidentialité et à la protection de la vie privée. L'enjeu se concentre donc sur le trajet emprunté par les données pendant leur utilisation au cours du cycle de vie. Il n'est pas question de marquage.

S'il y avait des normes prévoyant un mécanisme pour la création de liens entre un nouvel élément d'information et l'élément auquel il fait référence (la relation entre les étiquettes de données), les propriétaires et utilisateurs sauraient d'où vient l'information et comment elle est utilisée, c'est-à-dire la chaîne de valeur des données.

La normalisation devrait jeter de la lumière sur les questions entourant le concept de transparence des métadonnées. Par exemple, la transparence s'applique-t-elle aussi à l'algorithme utilisé pour la collecte? (Les données d'un client de l'industrie bancaire peuvent servir à en produire d'autres; la transparence s'applique-t-elle à cette pratique utilisée pour modifier les données recueillies?)

En plus des questions de transparence susmentionnées, voici d'autres exemples de sujets que pourrait aborder un cadre normatif :

- Si le fournisseur envoie les données au consommateur, c'est une opération; si le consommateur transforme les données et les transmet à un autre consommateur, c'en est une autre.
- Si le propriétaire initial des données les reprend après leur utilisation, on présume qu'il s'agit d'un artefact. Un certain degré de transparence doit aussi s'appliquer à ces données reprises.

Lacune : Transparence, parcours et traçabilité des données. Selon l'analyse, la plupart des normes générées par la recherche ont été jugées de portée très restreintes et seulement utiles à certains secteurs.

D'autres recherches s'imposent sur des sujets tels que la validation, les pistes de vérification, la création de chaînes de valeur, les acteurs et la traçabilité des données dérivées, qui feraient intervenir différents aspects du trajet des données en lien avec l'enjeu.

Besoins en recherche et développement? Oui, sur les chaînes de valeur, la traçabilité des données dérivées et des chaînes de blocs, l'Internet des objets, l'identité numérique, les chaînes de suivi et les matrices RACI.

Recommandation : Utiliser une matrice RACI.

Degré de priorité : Moyen/Faible

Organisation(s) : ISO/IEC, CCIAN

Enjeu 29 – Portabilité et mobilité des données

Cet enjeu porte principalement sur la création d'un cadre d'interopérabilité des systèmes qui donne à l'utilisateur le contrôle sur ses propres renseignements, grâce à la non-catégorisation des éléments d'information et à l'extraction des données en format numérique, et qui permet d'échanger de l'information à des fins semblables sans la modifier explicitement.

Pour assurer la portabilité et la mobilité des données, il faut des directives techniques communes qui faciliteront leur transfert entre responsables, par exemple à l'aide d'un dispositif pouvant être transféré d'un téléphone cellulaire à un autre. Le droit à la portabilité des données donne aux personnes concernées accès aux renseignements personnels qu'elles ont fournis, dans un format structuré, couramment utilisé et lisible par machine, tout en permettant la transmission de ces données entre responsables. L'idée est de créer un cadre pour l'exportation de données en format détaillé, tout en maintenant la possibilité de contextualiser l'information et de décider où elle peut aller sans qu'il soit nécessaire de la réduire avant son utilisation.

Il est essentiel de maintenir les échanges d'information entre systèmes et machines de sorte que les données puissent être utilisées au même titre sans être explicitement transformées. Par exemple, dans le contexte d'opérations financières menées par le consommateur, la portabilité et la mobilité servent à introduire de nombreux services de gestion numérique, puisqu'elles donnent accès aux données financières du consommateur. Une distinction doit être faite entre la portabilité et la mobilité, cette dernière ayant un effet sur l'utilisation des données.

Lacune : Portabilité et mobilité des données. Selon l'analyse, la plupart des normes générées par la recherche à ce sujet sont pertinentes. Fait intéressant : on remarque que la majorité des normes sont récentes, ce qui laisse croire que les organismes d'élaboration de normes travaillent déjà à combler les lacunes pour cet enjeu. De plus amples recherches aideraient à corriger le tir dans le domaine de la santé, où le transfert de dossiers entre systèmes n'est pas au même niveau que dans les autres secteurs.

Besoin en recherche et développement? Oui, sur les secteurs comme celui des soins de santé (portabilité des dossiers médicaux d'une province à l'autre) et la création d'une structure catégorielle pour les éléments d'information.

Recommandation : Discuter des moyens d'améliorer la disponibilité des outils de portabilité (plateformes communes de portabilité et de mobilité des données).

Degré de priorité : Moyen/Faible

Organisation(s) : ISO/IEC

Groupe de travail 4 : Analyses, solutions et commercialisation

Enjeu 30 – Éléments techniques des solutions d'IA

Cet enjeu concerne les éléments techniques des solutions d'IA (technologies, logiciels et plateformes). Il englobe la terminologie employée (y compris l'intelligence artificielle comme telle), les sous-catégories d'intelligence artificielle, la description du cycle de vie et chacune des composantes. Sont comprises dans sa portée les étapes d'analyse, de vérification et de validation du processus de sélection et d'utilisation des solutions et plateformes d'IA.

L'IA évolue rapidement; l'adoption d'un langage commun faciliterait les communications entre les autorités de réglementation, les innovateurs et les consommateurs. Beaucoup de définitions ont été proposées et publiées, mais elles ne font pas l'unanimité, et l'adoption des termes définis porte encore à confusion. De plus, il reste du travail à faire pour définir le cycle de vie de l'IA et particulièrement le cadre d'assurance de la qualité, non seulement du point de vue des politiques, mais aussi sous l'angle de l'analyse technique de vérification et de validation.

Ce domaine suscite beaucoup d'intérêt et d'activités dans les milieux réglementaires, industriels et normatifs. Le comité ISO/IEC JTC 1/SC 42 s'est notamment penché sur le cycle de vie de l'IA, ainsi que sur la meilleure façon d'en valider les composantes. Une approche sectorielle est aussi en cours d'élaboration; des travaux ont été lancés dans le secteur de la santé, sur l'utilisation de logiciels comme moyen d'intégrer l'IA dans les outils médicaux. Mais ce n'est encore que le début. Les possibilités continuent de se multiplier, et il faudra collaborer pour adopter une approche cohérente à l'échelle du pays.

Lacune : Éléments techniques des solutions d'IA. La recherche à ce sujet a généré un grand nombre de normes, mais la plupart n'étaient pas pertinentes, et de celles qui l'étaient, certaines ne traitaient qu'indirectement de l'enjeu ou relevaient d'un secteur précis, notamment la santé et les transports. On note l'absence de normes visant une catégorie d'intervenants, ceux de la fonction publique. Le petit nombre de normes directement liées à l'enjeu montre que la normalisation à cet égard ne fait que commencer. En effet, plusieurs normes sont en cours d'élaboration. Ce constat est confirmé par le fait que plus d'un tiers des normes étudiées datent de 2015 ou après.

Besoins en recherche et développement? Oui

Recommandation : Poursuivre les initiatives de normalisation pour favoriser l'élaboration et la mise en œuvre de solutions d'IA. Celles-ci sont en constante évolution, et l'innovation dans ce domaine ne cesse de repousser les limites. La recherche et le développement sur le sujet occupent une place importante au Canada et devraient continuer de donner naissance à de nouvelles technologies.

Degré de priorité : Élevé/Moyen

Organisation(s) : Organisations du secteur de l'intelligence artificielle, organismes de réglementation des provinces et territoires et du gouvernement fédéral, OEN internationaux

Enjeu 31 – Chaînes de valeur des données

Cet enjeu concerne la monétisation (en tant que cadre pour la création de nouvelles chaînes de valeur des actifs de données) et le rôle de la propriété intellectuelle dans la gestion des données.

Ce domaine doit être mieux défini. La plupart des initiatives actuelles se concentrent sur la description du cycle de vie des données. Bien qu'il y ait un consensus sur l'importance de l'évaluation des données, particulièrement lors de l'échange, il n'y a aucune ligne directrice, ou presque, sur ce processus, ni de cadre pour la création de nouvelles chaînes de valeur. Il serait donc nécessaire de mieux structurer la description de la monétisation et les méthodes liées aux opérations efficaces et équitables pour tous.

Lacune : Chaînes de valeur des données. La recherche n'a pas généré beaucoup de normes à ce sujet. Certains secteurs en ont, comme ceux du transport et de la santé, et certaines normes portent en particulier sur la valeur des données et la collecte dans les villes intelligentes. Il manque toutefois de normes dans le secteur financier. Il y en a beaucoup sur la portabilité et le stockage dans les applications de chaînes de blocs, mais aucune d'entre elles ne touche à l'intelligence artificielle. Les mots clés compris dans la recherche ont généré des normes sur la gouvernance des données en général. Il est à noter que plus d'un tiers des normes étudiées dataient de 2015 ou après, preuve qu'un grand courant de normalisation existe pour cet enjeu.

Besoins en recherche et développement? Oui

Recommandation : Concevoir des cadres, des directives sur la création de chaînes de valeur des données dans divers secteurs et des stratégies pour l'échange d'information. Il faudrait préciser que cet enjeu devra être revu à mesure que les données gagnent en importance.

Degré de priorité : Moyen/Faible

Organisation(s) : OEN nationaux, régionaux et internationaux.

Enjeu 32 – Transparence et communication des analyses de données

Cet enjeu couvre la communication des analyses de données, de même des risques pour les propriétaires de données, du point de vue de la chaîne d'approvisionnement. Nous avons préféré le terme « transparence » au terme « divulgation » dans le nom de l'enjeu, à cause de la possible connotation juridique du second. L'enjeu porte sur la façon de communiquer les risques et processus, ainsi que sur la transparence prévue pour les utilisateurs et les propriétaires de données.

Certains se demandent dans quelle mesure le niveau d'analyse des données est divulgué et communiqué aux propriétaires et à l'ensemble des consommateurs. Cette question reste toujours sans réponse, et si des cas anecdotiques sont repris par les médias ou soulevés par certaines autorités de réglementation, les solutions coordonnées manquent pour une communication adéquate. Lorsqu'une personne accepte de fournir des informations, elle n'est pas informée immédiatement et clairement du risque que ces informations servent à l'identifier à court ou à long terme. Les connaissances et les structures manquent quant à la façon de communiquer les différents niveaux de risque. Il faut également tenir compte du public cible pour établir la portée de la communication; en effet, le niveau de transparence et de communication peut varier selon les destinataires de l'information (fournisseurs, autorités de réglementation, tiers ou clients).

La collecte de données au cœur de la pandémie de COVID-19 constitue un exemple très actuel du problème. La multiplication des collectes de données sur la santé, associée aux considérations sur le suivi des déplacements, crée un risque. Des discussions ont été entreprises sur la création d'une « étiquette nutritionnelle » pour les données afin d'en améliorer la clarté. Une telle étiquette contribuerait à faire connaître les métadonnées créées, les cadres utilisés et le vocabulaire normalisé. Une autre avenue réside dans l'élaboration de fiches techniques pour les jeux de données. Certains demandent la création d'une hiérarchie des niveaux de communication en fonction du degré de confidentialité. Les renseignements personnels font aussi l'objet de préoccupations, aussi bien chez les propriétaires des données que chez les analystes. Des initiatives réglementaires ont été lancées à ce sujet, les mieux connues étant les travaux de la Commission européenne ayant mené au *Règlement général sur la protection des données*. Des exemples de cet enjeu ont été soulevés dans le secteur financier et celui de l'énergie. Le degré de transparence des transactions financières joue un rôle important dans la détection du blanchiment d'argent et de la fraude, mais suscite également des inquiétudes quant à la protection des renseignements personnels du public. La Commission de l'énergie de l'Ontario s'est penchée sur le niveau de transparence à viser concernant la consommation d'énergie dans ses communications en ligne et sa réglementation. À l'échelle municipale, mentionnons le projet Sidewalk Labs de Toronto : aujourd'hui terminé, il avait donné lieu à un ensemble d'icônes correspondant aux différents types de données recueillies.

Dans ses discussions, le groupe de travail a cerné ainsi certaines notions :

Propriété (des données)

- Propriété publique ou individuelle de renseignements personnels :
  - communiqués à dessein (ex. : test d'ADN, achat par carte de crédit ou carte fidélité);
  - communiqués inconsciemment (ex. : caméra en circuit fermé, reconnaissance faciale);
  - dans le domaine public.
- Propriété commerciale de données recueillies
- Propriété gouvernementale de données recueillies
- Propriété universitaire de données recueillies

Collecte (des données)

- Saisie initiale des données
- Utilisation de banques de données existantes
- Anonymisation/désagrégation des données (ex. : applis COVID)

Intendance (des données)

- Maintien de la qualité et de l'accessibilité et stockage des données
- Tenue à jour de la liste d'utilisateurs et de destinataires des données pour un suivi régulier
- Formation des utilisateurs sur la reconnaissance des biais inconscients ou implicites
- Élaboration et prestation de formations sur les biais adaptées à divers types d'utilisateurs (opérations, politiques, stratégies ou techniques)
- Définition d'approches visant à régler différents types de problèmes de données (opérationnels, politiques, stratégiques ou techniques) – Aucune solution universelle
- Maintien de la capacité pour un propriétaire de données de les retirer ou d'annuler son consentement à leur utilisation (ex. Google, archives Twitter de la Library of Congress)

- Maintien de la désagrégation et de l'anonymisation des données
- Suivi du processus décisionnel et des interactions entre les systèmes

Utilisation (des données)

- Organisation, gouvernement, université, entité indépendante ou individu
- Répercussions des droits des chercheurs sur les renseignements personnels

Gouvernance (des données)

- Surveillance et correction de la portée ou du glissement de portée pour un utilisateur ou un système (les données utilisées pour résoudre un problème doivent correspondre à celui-ci)
- Définition/mise à jour de lignes directrices sur la gestion de partage d'information entre systèmes (sans intervention humaine)
- Définition des conséquences financières des intrusions ou des biais
- Détermination de la valeur des données recueillies
- Détermination de la probabilité, de la classification, de la cartographie, des seuils et de l'atténuation des risques pour les données et les systèmes, ainsi que de la propension au risque
- Gouvernance dans les organisations et l'industrie, pratiques exemplaires et réglementation/législation

Lacune : Transparence et communication des analyses de données. Selon la description de certains enjeux connexes, il est possible que les normes trouvées par d'autres groupes de travail soient utiles pour l'étude du présent enjeu. La recherche sur ce dernier a permis de trouver de nombreuses normes; cependant comme les mots-clés utilisés n'ont souvent pas le même sens dans ces normes que dans la description de l'enjeu, nombre d'entre elles ne s'appliquent pas. Plusieurs des normes correspondant au niveau II seraient utiles pour explorer des possibilités d'élaboration de normes de niveau I. Un certain nombre de normes sectorielles pourraient aussi s'appliquer, même si leur domaine d'application est restreint.

Besoins en recherche et développement? Oui

Recommandation : Encourager les Canadiens à poursuivre la discussion, à mieux comprendre et définir les répercussions de cet enjeu, et à participer à l'élaboration de normes dans le domaine. Il est nécessaire d'explorer davantage cet enjeu et de lancer une discussion élargie sur la façon dont ses différents aspects sont perçus et sur certaines des approches utilisées par les intervenants au Canada et à l'étranger.

Degré de priorité : Élevé

Organisation(s) : Organisations du secteur de l'intelligence artificielle, organismes de réglementation des provinces et territoires et du gouvernement fédéral, OEN internationaux

Enjeu 33 – Interprétabilité et clarté des systèmes d'IA

(D'abord appelé « Interprétabilité des algorithmes »)

Cet enjeu traite de la transparence des capacités et des fonctions d'un algorithme. Étant donné l'ampleur et le rythme des innovations, il faut établir un niveau minimal d'exigences pour garantir l'interprétabilité des solutions et des produits créés par des outils avancés d'analyse des données et assurer une certaine stabilité dans l'élaboration de nouvelles applications pour différents secteurs.

L'accent est mis sur le manque de clarté des algorithmes. Il y a un conflit apparent entre le besoin de transparence et le fait que l'innovation réside dans la capacité d'adaptation et d'évolution en cours d'analyse. C'est d'autant plus difficile lorsqu'il s'agit d'un système complexe pouvant comporter des algorithmes qui fournissent des recommandations pour la prise de décision. Dans les secteurs très réglementés, il devient ardu de démontrer aux autorités de réglementation que les cadres en vigueur sont suivis.

Lacune : Interprétabilité et clarté des systèmes d'IA. Les mots-clés choisis pour cet enjeu ont permis de trouver de nombreuses normes, mais aucune ne correspond au niveau I. La plupart des normes trouvées utilisent les mots-clés dans un contexte différent. Certaines d'entre elles correspondent au niveau II et portent sur des aspects de l'enjeu du point de vue de la gestion du risque en technologie de l'information. De nouvelles normes (sectorielles et générales) sont nécessaires dans ce domaine pour répondre aux besoins exprimés par les intervenants.

Besoins en recherche et développement? Oui

Recommandation : Poursuivre les activités de recherche et développement dans ce secteur pour étoffer les applications des mots-clés. Par la suite, les innovateurs canadiens devraient participer aux initiatives de normalisation au fur et à mesure qu'elles verront le jour.

Degré de priorité : Moyen

Organisation(s) : OEN nationaux, régionaux ou internationaux

Enjeu 34 – Évaluation et gestion des biais

La détection des biais et leur prise en compte constituent un enjeu central. Le terme « biais » désigne une différence systématique dans la manière de traiter (perception, observation, représentation, prédiction, décision, etc.) certains objets, individus ou groupes comparativement à d'autres. Cet enjeu est lié à celui de la gestion de la performance des systèmes, mais nous l'avons traité à part pour pouvoir nous concentrer sur ses aspects complexes et délicats.

Les solutions et recommandations fournies par les algorithmes et outils d'analyse de données ont des effets sur la vie quotidienne des gens. Il faut donc scruter attentivement la façon dont ces solutions et recommandations sont mises en œuvre, ainsi que les facteurs qui en influencent les répercussions. Lorsque ces solutions et recommandations touchent la vie en société, il importe de voir si des idées préconçues ont teinté le processus. Certaines technologies sont volontairement conçues avec certains biais; il faut se pencher sur la façon d'en tenir compte lorsqu'on les utilise. Les risques peuvent avoir des conséquences très sérieuses; c'est pourquoi nous avons traité cet enjeu séparément.

Les médias ont rapporté de nombreux cas de systèmes d'IA incluant des biais. On a vu des articles de presse sur les recommandations racistes formulées par de tels systèmes sur les taux de récidive aux États-Unis, à cause de biais résultant d'une longue histoire de préjugés au sein des forces de l'ordre. Certains s'inquiètent du fait que des décisions médicales ou financières s'appuieraient sur des résultats influencés par une perspective discriminatoire ou un ensemble incomplet de données démographiques. Les biais sont très probables quand la décision se base sur des caractéristiques non pertinentes comme l'apparence (ex. : primes d'assurance plus chères pour les jeunes), mais on peut se demander si c'est le cas lorsque ces décisions sont exclusivement basées sur des données, comme le plus grand nombre d'accidents chez les jeunes. Récemment, les possibles conséquences discriminatoires de la reconnaissance faciale ont été soulignées dans les médias.

Cet enjeu résulte de l'adoption étendue d'outils technologiques et novateurs. Les travaux se poursuivent, et au fur et à mesure qu'ils seront adoptés, de nouvelles questions et de nouvelles solutions émergeront. Soulignons qu'il est inexact et implicitement discriminatoire de présumer et d'affirmer qu'un ensemble de données ou un système est exempt de tout biais sans en avoir de preuve validée par un expert.

Les biais tels que décrits par les groupes de travail 1 et 2 ont été exclus de la portée de cet enjeu.

Lacune : Évaluation et gestion des biais. Les mots-clés sélectionnés pour cet enjeu ont ramené peu de normes, et aucune ne correspondait au niveau I. La majorité d'entre elles utilisent les mots-clés dans un contexte différent. Une norme en particulier, correspondant au niveau II, porte sur la question de la fiabilité, dont il est question aux sections ci-dessus sur les biais. De nouvelles normes (sectorielles et générales) sont nécessaires dans ce domaine pour répondre aux besoins exprimés par les intervenants.

Besoins en recherche et développement? Oui

Recommandation : Normaliser les protocoles, les processus et les évaluations qui servent à recenser les biais et normaliser, s'il y a lieu, les mécanismes qui les encadrent.

Degré de priorité : Moyen

Organisation(s) : OEN nationaux, régionaux ou internationaux

Enjeu 35 – Systèmes de gestion de la performance des outils d'analyse et des systèmes d'IA

Cet enjeu est axé sur la gouvernance interne, à partir de l'analyse du niveau de risque jusqu'à la conception et au déploiement de modèles, d'algorithmes et de systèmes. Il porte sur l'ensemble de la gestion de la performance, et notamment sur la façon de gérer toute interaction avec les humains. Il couvre aussi l'analyse de l'utilisation des normes sur les systèmes de management dans l'univers de l'intelligence artificielle, la méfiance et le manque de lignes directrices entourant le déploiement et l'utilisation des systèmes d'IA, des algorithmes et des modèles d'analyse de données dans les organisations existantes, de même que la façon dont les consommateurs et les utilisateurs finaux évaluent les cadres actuels.

Au fur et à mesure que le secteur se développe, il faut aller vers une gouvernance de l'IA fondée sur le risque, c'est-à-dire que les organisations doivent pouvoir gérer les questions de performance en fonction de leur « profil de risque ». Cette nécessité est se confirme dans des normes en cours de rédaction, comme la norme ISO/IEC 38507, *Technologies de l'information – Gouvernance des technologies de l'information – Implications de gouvernance de l'utilisation par des organisations de l'intelligence artificielle*. Par ailleurs, un mouvement de plus en plus important prône l'élaboration d'une norme qui définirait des exigences et fournirait des lignes directrices pour la création, la mise en place, la tenue à jour et l'amélioration continue d'un système de gestion de l'intelligence artificielle dans le contexte d'une organisation. Une telle norme répondrait à un besoin de gouvernance dans la gestion de la performance, tous secteurs confondus, tout en jetant les bases de la réponse future aux besoins sectoriels.

Lacune : Systèmes de gestion de la performance des outils d'analyse et des systèmes d'IA. La recherche a permis de trouver un certain nombre de normes. La majorité d'entre elles ne correspondent pas aux mots-clés ou à l'enjeu tel que décrit. Les autres étaient soit des normes générales sur le management ou la gouvernance, soit des normes axées sur des secteurs traditionnels. Certaines normes, même si elles ne s'appliquent pas à l'enjeu, constitueraient de bonnes références dans l'élaboration de normes de niveau I.

Besoins en recherche et développement? Oui

Recommandation : La gouvernance et la gestion de la performance vont de pair avec la maturation d'une technologie. Elles continueront d'évoluer au fur et à mesure que la technologie se développe et que les applications se multiplient dans ce secteur. Nous n'avons pas cerné de besoin particulier en recherche et développement. Des intervenants de divers horizons et secteurs devraient participer aux activités de normalisation dans ce domaine.

Degré de priorité : Moyen

Organisation(s) : Associations sectorielles en IA, organismes de réglementation des provinces et territoires et du gouvernement fédéral, OEN internationaux

Annexe B –

Liste de normes publiées de niveau 1 et des documents connexes pour les questions clés

Groupe de travail 1 : Foundements de la gouvernance des données

Question clé 1 cadre de responsabilité

IEEE STDVA24228	[Disponible uniquement en anglais]
ISO/TR 24514	Activités relatives aux services de l'eau portable et de l'assainissement – exemples d'utilisation d'indicateurs de performance à l'aide l'ISO 24510, l'ISO 24511 et l'ISO 24512 et des méthodologies associées
ETSI TR 103 591	[Disponible uniquement en anglais]
CSA PLUS 8830-95	[Disponible uniquement en anglais]
SAE GEIA-HB-859	[Disponible uniquement en anglais]
ISO/IEC 22624	[Disponible uniquement en anglais]
ETSI SR 003 391	[Disponible uniquement en anglais]
ITU-T H.860	Services d'échange de données multimédias concernant la cybersanté : schéma des données et services support
ITU-T Y.3514	Informatique en nuage – Cadre et exigences concernant la confiance pour les échanges inter-nuages
CEN/TR 17370	[Disponible uniquement en anglais]
ISO 11240	Informatique de santé – identification des médicaments – éléments de données et structures pour l'identification unique et l'échange d'informations sur les unités
ISO 15394	Emballage – codes à barres et symboles bidimensionnels pour l'expédition, le transport et les étiquettes de réception
ISO/IEC 20748.4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4
ISO/IEC 24760-2	Technologies de l'information – Techniques de sécurité – cadre pour la gestion de l'identité – Partie 2 : Architecture de référence et exigences
ISO/IEC 29151	Technologies de l'information – Techniques de sécurité – code de bonne pratique pour la protection des données à caractère personnel

ISO/IEC 29187-1	Technologies de l'information – Identification des exigences de protection privée concernant l'apprentissage, l'éducation et la formation (AÉF) – Partie 1 : Cadre Général et Modèle de Référence
ISO/IEC TS 20748-4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4
DIN SPEC 4997	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO/IEC 29184:2020	Technologies de l'information – Déclarations de confidentialité en ligne et les consentements
ISO/IEC WD TS 27560	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 103-1:2020	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2
IEEE P7002	[Disponible uniquement en anglais]
IEEE P7004	[Disponible uniquement en anglais]
IEEE P7005	[Disponible uniquement en anglais]
IEEE P2089	[Disponible uniquement en anglais]
IEEE P3800	[Disponible uniquement en anglais]
IEEE P2895	[Disponible uniquement en anglais]
IC16-002	[Disponible uniquement en anglais]
IC19-004	[Disponible uniquement en anglais]
IC18-004	[Disponible uniquement en anglais]

Question clé 2
certification pour les rôles professionnels

ETSI TR 103 370	Guide introductif pratique aux normes techniques en matière de confidentialité
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
COBIT 2019	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes sur la finance destinée aux consommateurs (Open Banking)
CIOSC 102	Qualification et certification du personnel en matière de mégadonnées et d'apprentissage machine
CAN/CIOSC 109-1	Qualification et compétence des professionnels du contrôle de la confidentialité et de l'accès aux renseignements
ISO/IEC/IEEE 24765:2017	Ingénierie des systèmes et du logiciel – Vocabulaire

Question clé 3
habileté numérique

ITU-T L.1505	Technologies de l'information et de la communication et adaptation du secteur de la pêche aux effets des changements climatiques
ISO 21248	Information et documentation – Évaluation de qualité pour les bibliothèques nationales
ISO/IEC TR 18120	Technologies de l'information – Apprentissage, éducation et formation – Exigences pour les livres de texte électroniques dans l'éducation
ISO/IEC 18120	Technologies de l'information – Apprentissage, éducation et formation – Exigences pour les livres de texte électroniques dans l'éducation
ISO/IEC 19788-5	Technologies de l'information – Apprentissage, éducation et formation – Métadonnées pour ressources d'apprentissage – Partie 5 : Éléments pédagogiques
ISO/IEC TR 18120	Technologies de l'information – Apprentissage, éducation et formation – Exigences pour les livres de texte électroniques dans l'éducation
BSI PAS 1040	[Disponible uniquement en anglais]
BSI PAS 1296	[Disponible uniquement en anglais]
ISO/TR 14639-2	Informatique de santé – Feuille de route de l'architecture de santé électronique fondée sur la capacité – Partie 2 : Composants architecturaux et modèle de maturité
DS DS/CWA 16213	[Disponible uniquement en anglais]
DS DS/CWA 16266	[Disponible uniquement en anglais]

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	Elements d'IA
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes sur la finance destinée aux consommateurs (Open Banking)
IEEE 3527.1-2020	[Disponible uniquement en anglais]
IEEE P2089	[Disponible uniquement en anglais]
IEEE P7011	Procédé de Tirage d'Identification et d'Évaluation de la Sécurité de Sources de Nouvelles

Question clé 4
protection de la cybersécurité

ISO/IEC 29100	Technologies de l'information – Techniques de sécurité – Cadre privé)
ISO/IEC TR 27103	Technologies de l'information – Techniques de sécurité – Cybersécurité et normes ISO et IEC
CEN/TS 17288	[Disponible uniquement en anglais]
ETSI TR 103 591	[Disponible uniquement en anglais]
CENELEC EN 50584	[Disponible uniquement en anglais]

CENELEC EN 50173-1	Technologies de l'information – Systèmes de câblage générique – Partie 1 : Exigences générales
CENELEC EN 50173-2	Technologies de l'information – Systèmes de câblage générique – Partie 2 : Espaces de bureau
CENELEC EN 50173-5	Technologies de l'information – Systèmes de câblage générique – Partie 5 : Espaces de centres de traitement de données
ISO/IEC 8348	Technologies de l'information – Interconnexion de systèmes ouverts OSI – Définition du service de réseau
ISO/IEC 17788	Technologies de l'information – Informatique en nuage – Vue d'ensemble et vocabulaire
ISO/IEC 17789	Technologies de l'information – Informatique en nuage – Architecture de référence
ITU-T Y.3500	[Disponible uniquement en anglais]
ITU-T Y.3502	Technologies de l'information – Informatique en nuage – Architecture de référence
ISO/IEC 15504.5	Technologies de l'information – Évaluation des procédés – Partie 5 : Un exemple de modèle d'évaluation des procédés du cycle de vie d'un logiciel
ISO/IEC 15504-5	Technologies de l'information – Évaluation des procédés – Partie 5 : Un exemple de modèle d'évaluation des procédés du cycle de vie d'un logiciel
ISO/IEC 18028.2	Technologies de l'information – Techniques de sécurité – Sécurité de réseaux TI – Partie 2 : Architecture de sécurité de réseau
ISO/IEC 19770-8	[Disponible uniquement en anglais]
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 24760-2	Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 2 : Architecture de référence et exigences
ISO/IEC 27034-5	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SECURITE – SECURITE DES APPLICATIONS – PARTIE 5 : PROTOCOLES ET STRUCTURE DE DONNÉES DE CONTRÔLES DE SÉC
ISO/IEC 27050-1	TECHNOLOGIES DE L'INFORMATION – DÉCOUVERTE ÉLECTRONIQUE – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 29101	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – ARCHITECTURE DE RÉFÉRENCE DE LA PROTECTION DE LA VIE PRIVÉE
ISO/IEC 29115	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CADRE D'ASSURANCE DE L'AUTHENTIFICATION D'ENTITÉ
ISO/IEC 29190	Technologies de l'information – Techniques de sécurité – Modèle d'évaluation de l'aptitude à la confidentialité
ISO/IEC 30100-2	[Disponible uniquement en anglais]
ISO/IEC 30105-2	TECHNOLOGIES DE L'INFORMATION – PROCESSUS DU CYCLE DE VIE DE LA DÉLOCALISATION DU PROCESSUS D'AFFAIRES DES SERVICES ACTIVÉS PAR IT – PARTIE 2 : MODÈLE D'ÉV
ISO/IEC 38500	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION POUR L'ENTREPRISE
ISO/IEC 38505-1	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des do
ISO/IEC 38506	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – APPLICATION DE L'ISO/IEC 38500 À LA GOUVERNANCE DES INVESTISSEMENTS
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC TS 27034-5-1	Technologies de l'information – Sécurité des applications – Partie 5-1 : Protocoles et structure de données de contrôles de sécurité d'application, schémas XML
SNZ AS/NZS 15271	[Disponible uniquement en anglais]
CEN EN 16571	Technologies de l'information – Processus d'évaluation d'impact sur la vie privée des applications RFID
ISO/IEC/IEEE 42030	Logiciel, systèmes et entreprise – Cadre d'évaluation de l'architecture
CENELEC EN 50667	Technologie de l'information – Systèmes de gestion d'infrastructure automatisée (AIM, Automated infrastructure management) – Exigences, échange de données et applications

ISO/IEC 18028-5	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE RÉSEAUX TI – PARTIE 5 : COMMUNICATIONS SÛRES À TRAVERS LES RÉSEAUX UTILISANT LES RÉSE
ISO/IEC 18043	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉLECTION, DÉPLOIEMENT ET OPÉRATIONS DES SYSTÈMES DE DÉTECTION D'INTRUSION
ISO/IEC 20243-2	TECHNOLOGIES DE L'INFORMATION – NORME DE FOURNISSEUR DE TECHNOLOGIE DE CONFIANCE OUVERTE (O-TTPS) – ATTÉNUATION DES PRODUITS CONTREFAITS ET MALICIEU
ISO/IEC 21878	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR LA CONCEPTION ET L'IMPLÉMENTATION SÉCURISÉES DES SERVEURS VIRTUALISÉS
ISO/IEC 24760-3	Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 3 : Mise en œuvre
ISO/IEC 27034-1	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DES APPLICATIONS – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 27034-2	TECHNOLOGIE DE L'INFORMATION – SÉCURITÉ DES APPLICATIONS – PARTIE 2 : CADRE NORMATIF DE L'ORGANISATION
ISO/IEC 27034-3	Technologie de l'information – Sécurité des applications – Partie 3 : Processus de gestion de la sécurité d'une application
ISO/IEC 27039	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉLECTION, DÉPLOIEMENT ET OPÉRATIONS DES SYSTÈMES DE DÉTECTION ET PRÉVENTION D'INTRUSION
ISO/IEC 29134	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR L'ÉTUDE D'IMPACTS SUR LA VIE PRIVÉE
ISO/IEC TR 13335-5	TECHNOLOGIES DE L'INFORMATION – LIGNES DIRECTRICES POUR LA GESTION DE SÉCURITÉ IT – PARTIE 5 : GUIDE POUR LA GESTION DE SÉCURITÉ DU RÉSEAU
ISO/IEC TR 14516	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR L'UTILISATION ET LA GESTION DES SERVICES DE TIERS DE CONFIANCE
ISO/IEC TR 15443-1	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – ASSURANCE DE LA SÉCURITÉ CADRE – PARTIE 1 : INTRODUCTION ET CONCEPTS
ISO/IEC TR 15443-2	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – ASSURANCE DE LA SÉCURITÉ CADRE – PARTIE 2 : ANALYSES
ISO/IEC TR 15443-3	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – UN CANEVAS POUR L'ASSURANCE DE LA SÉCURITÉ DANS LES TECHNOLOGIES DE L'INFORMATION – PARTIE 3 :
ISO/IEC TR 19791	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – ÉVALUATION DE LA SÉCURITÉ DES SYSTÈMES OPÉRATIONNELS
ISO/IEC TR 27550	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – INGÉNIERIE DE LA VIE PRIVÉE POUR LES PROCESSUS DU CYCLE DE VIE DES SYSTÈMES
ISO/IEC TR 29156	TECHNOLOGIES DE L'INFORMATION – DIRECTIVES SPÉCIFIANT LES EXIGENCES DE PERFORMANCE AFIN D'ATTEINDRE LA SÉCURITÉ ET LES BESOINS D'UTILISATION DANS LES APPLIC
ISO/IEC TR 29181-5	TECHNOLOGIES DE L'INFORMATION – RÉSEAUX DU FUTUR – ÉNONCÉ DU PROBLÈME ET EXIGENCES – PARTIE 5 : SÉCURITÉ
ITU-T STIT	[Disponible uniquement en anglais]
ITU-T X.842	Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'utilisation et à la gestion des services de tiers de confiance
ISO/IEC 27006	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – EXIGENCES POUR LES ORGANISMES PROCÉDANT À L'AUDIT ET À LA CERTIFICATION DES SYSTÈMES DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION – AMENDEMENT 1
ITU-T SERIES Y SUPP 49	[Disponible uniquement en anglais]
DIN SPEC 91367	[Disponible uniquement en anglais]
ISO 14641	ARCHIVAGE ÉLECTRONIQUE – CONCEPTION ET EXPLOITATION D'UN SYSTÈME INFORMATIQUE POUR LA CONSERVATION INTÈGRE DE DOCUMENTS ÉLECTRONIQUES – SPÉCIFICATIONS
ISO 29134	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR L'ÉTUDE D'IMPACTS SUR LA VIE PRIVÉE

ISO/IEC 10021-8	TECHNOLOGIES DE L'INFORMATION – SYSTÈMES DE MESSAGERIE (MHS) – PARTIE 8 : SERVICE DE MESSAGERIE PAR ÉCHANGE INFORMATISÉ DE DONNÉES
ISO/IEC 18045	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – MÉTHODOLOGIE POUR L'ÉVALUATION DE SÉCURITÉ TI
ISO/IEC 20944-1	TECHNOLOGIES DE L'INFORMATION – INTEROPÉRABILITÉ ET LIAISONS DES REGISTRES DE MÉTADONNÉES (MDR-IB) – PARTIE 1 : CADRE D'APPLICATIONS, VOCABULAIRE COMMUN ET DISPOSITIONS COMMUNES DE CONFORMITÉ
ISO/IEC 23736-3	TECHNOLOGIES DE L'INFORMATION – PUBLICATIONS NUMÉRIQUES – EPUB 3.0.1 – PARTIE 3 : DOCUMENTS DE CONTENU
ISO/IEC 27034-6	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DES APPLICATIONS – PARTIE 6 : ÉTUDES DE CAS
ISO/IEC 27034-7	TECHNOLOGIES DE L'INFORMATION – SÉCURITÉ DES APPLICATIONS – PARTIE 7 : CADRE DE L'ASSURANCE D'UNE PRÉDICTION
ISO/IEC 29147	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – DIVULGATION DE VULNÉRABILITÉ
ISO/IEC 30111	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – PROCESSUS DE TRAITEMENT DE LA VULNÉRABILITÉ
ISO/IEC TS 19249	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CATALOGUE DES PRINCIPES ARCHITECTURAUX ET CONCEPTUELS POUR LA SÉCURISATION DES PRODUITS, SYSTÈMES ET APPLICATIONS
ISO/IEC TS 20540	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – TEST DE MODULES CRYPTOGRAPHIQUES DANS LEUR ENVIRONNEMENT D'EXPLOITATION
ISO/IEC TS 22237-6	TECHNOLOGIE DE L'INFORMATION – INSTALLATION ET INFRASTRUCTURES DE CENTRES DE TRAITEMENT DE DONNÉES – PARTIE 6 : SYSTÈMES DE SÉCURITÉ
ISO/IEC 27033-5	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE RÉSEAU – PARTIE 5 : SÉCURITÉ DES COMMUNICATIONS AU TRAVERS DES RÉSEAUX UTILISANT DES

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

n/a	Stratégie nationale de cybersécurité
ISO 20252:2019	Études de marché, études sociales et d'opinion, y compris insights et analytique de données – Vocabulaire et exigences de service
ISO 19092:2008	Services financiers – Biométrie – Cadre de sécurité
ISO/TR 22100-4:2018	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes sur la finance destinée aux consommateurs (Open Banking)
CAN/CIOSC 100-1:2020	Gouvernance de données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance de données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CIOSC/PAS 100-4:2020	Gouvernance de données – Partie 4 : Spécification pour une infrastructure adaptable d'accès à distance
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 100-8	Gouvernance des données-Partie 8 : Cadre de géorésidence et de souveraineté
CAN/CIOSC 103-3	Confiance et identité numérique – Partie 3 : Justificatifs d'identité numériques
CAN/CIOSC 103-4	Confiance et identité numérique – Partie 4 : Portefeuilles
CAN/CIOSC 104	Contrôles de cybersécurité de base pour les petites et moyennes organisations

CAN/CIOSC 105	Cybersécurité des appareils et systèmes connectés à l'Internet industriel des objets (IIoT)
IEEE P2658	[Disponible uniquement en anglais]
IEEE P1547.3	[Disponible uniquement en anglais]
IEEE P2808	[Disponible uniquement en anglais]
IEEE P9274.4.2	[Disponible uniquement en anglais]
IEEE P2418.9	[Disponible uniquement en anglais]
IEEE P2933	[Disponible uniquement en anglais]
IEEE P1609.2	[Disponible uniquement en anglais]
IEEE P802.15.4y	[Disponible uniquement en anglais]
IEEE P802.1AEdk	[Disponible uniquement en anglais]
IEEE P1912	[Disponible uniquement en anglais]
IEEE P2621 series	[Disponible uniquement en anglais]
IEEE P1711.1	[Disponible uniquement en anglais]
IEEE P1686	[Disponible uniquement en anglais]
IEEE 2030.102.1-2020	[Disponible uniquement en anglais]
ISO/IEC 27400	[Disponible uniquement en anglais]
ISO/IEC 27402	[Disponible uniquement en anglais]
ISO/IEC 27403	[Disponible uniquement en anglais]
CSA T100**	[Disponible uniquement en anglais]
CSA T200**	[Disponible uniquement en anglais]
CSA EXP 200	[Disponible uniquement en anglais]
CSA T2000-1**	[Disponible uniquement en anglais]
CSA T2000-2**	[Disponible uniquement en anglais]
CSA Z246.1	Gestion de la sûreté des installations liées à l'industrie du pétrole et du gaz naturel – quatrième édition
CSA N290.7	Cybersécurité pour les centrales nucléaires et les installations dotées de petits réacteurs – Première édition
CSA T150**	[Disponible uniquement en anglais]
CSA T710**	[Disponible uniquement en anglais]
CAN/CSA-ISO 14971	[Disponible uniquement en anglais]
CAN/CSA-CEI/IEC 62304	[Disponible uniquement en anglais]

Question clé 5
gouvernance de la gestion des données

ISO/IEC TR 38505-2:19	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO 19731	Analytique numérique et analyses web pour les besoins d'études de marché, études sociales et d'opinion – Vocabulaire et exigences de service
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO 28500:2017	Information et documentation – Format de fichier WARC
ISO/IEC 38500:2015	Technologies de l'information – Gouvernance des technologies de l'information pour l'entreprise

ISO/IEC 38505-1:2017	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes sur la finance destinée aux consommateurs (Open Banking)
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-2:2020	Gouvernance des données – Partie 2 : Accès aux données et confidentialité
CAN/CIOSC 104	Contrôles de cybersécurité de base pour les petites et moyennes organisations
ISO/IEC/IEEE 42020:2019(E)	Logiciel, systèmes et entreprise – Processus d'architecture
ISO/IEC/IEEE 24765:2017	Ingénierie des systèmes et du logiciel – Vocabulaire
CSA T100**	[Disponible uniquement en anglais]
CSA T200**	[Disponible uniquement en anglais]
CSA EXP 200	[Disponible uniquement en anglais]
CSA T2000-1**	[Disponible uniquement en anglais]
CSA T2000-2**	[Disponible uniquement en anglais]
CSA Z246.1	Gestion de la sûreté des installations liées à l'industrie du pétrole et du gaz naturel – quatrième édition
CSA N290.7	Cybersécurité pour les centrales nucléaires et les installations dotées de petits réacteurs – Première édition
CSA T150**	[Disponible uniquement en anglais]
CSA T710**	[Disponible uniquement en anglais]
Z1635**	[Disponible uniquement en anglais]
CSA Z8000	Établissements de santé canadiens – deuxième édition

Question clé 6
protection des renseignements personnels

ANSI X9.42	[Disponible uniquement en anglais]
ANSI X9.63	[Disponible uniquement en anglais]
ANSI X9.73	[Disponible uniquement en anglais]
ANSI X9.84	[Disponible uniquement en anglais]
ANSI INCITS 446	[Disponible uniquement en anglais]
ASA S12.70	[Disponible uniquement en anglais]
ASCE GSP 226	[Disponible uniquement en anglais]
ASTM E2369	[Disponible uniquement en anglais]
ASTM E2147	[Disponible uniquement en anglais]
ASTM E2468	[Disponible uniquement en anglais]
ASTM E2259 REV A	[Disponible uniquement en anglais]
BSI BS 10102-1	[Disponible uniquement en anglais]
CEN EN 14302	[Disponible uniquement en anglais]
CEN EN 12924	[Disponible uniquement en anglais]
CEN EN 13608-3	[Disponible uniquement en anglais]

CEN/TR 16742	Systèmes de transport intelligents – Aspects de la vie privée dans les normes et les systèmes en Europe
CEN EN 15969-1	Citernes destinées au transport de matières dangereuses – Interface numérique pour le transfert de données entre des véhicules-citernes et des installations fixes – Partie 1 : Spécifications du protocole – Contrôle, données de mesure et d'événements
CEN EN 15969-2	Citernes destinées au transport de matières dangereuses – Interface numérique pour le transfert de données entre des véhicules-citernes et des installations fixes – Partie 2 : Données commerciales et logistiques
CEN EN 13032-1	Lumière et éclairage – Mesure et présentation des données photométriques des lampes et des luminaires – Partie 1 : Mesurage et format de données
CEN/TS 15430-2	Matériels de viabilité hivernale et d'entretien des dépendances routières – Acquisition et transmission des données – Partie 2 : Protocole de transfert de données entre le serveur fournisseur d'information et le serveur d'application client
CEN EN 13757-7	Systèmes de communication pour compteurs – Partie 7 : Services de transport et de sécurité
CENELEC EN 50491-11	Exigences générales pour systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) et pour systèmes de gestion technique du bâtiment (SGTB) – Partie 11 : Comptage intelligent – Spécifications d'application – Affichage simple et externe du client
CGSB CAN/CGSB-133.1-2017	Agents de sécurité et superviseurs des agents de sécurité
CAN/CIOSC 109-1	Qualification et maîtrise des professionnels de la confidentialité et du contrôle d'accès
CAN/CIOSC 109-2	Cadre canadien de protection de la confidentialité des informations
CLSI M39-A4	[Disponible uniquement en anglais]
CLSI AUTO10-A	[Disponible uniquement en anglais]
CLSI MM20-A	[Disponible uniquement en anglais]
CSA Q830	Code type sur la protection des renseignements personnels
CSA B480-02	Service à la clientèle adapté aux besoins des personnes handicapées
CSA B480-02 LARGE PRINT	Service à la clientèle adapté aux besoins des personnes handicapées
CSA CAN/ CSA-B651.2-07	Conception accessible des dispositifs interactifs libre-service
CSA PLUS 8830-95	[Disponible uniquement en anglais]
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN SPEC 91357	[Disponible uniquement en anglais]
ETSI TR 102 612	[Disponible uniquement en anglais]
ETSI TS 103 458	[Disponible uniquement en anglais]
ETSI TR 101 584	[Disponible uniquement en anglais]
ETSI EN 300 392-1 V1.6.1	[Disponible uniquement en anglais]
ETSI TR 103 603	[Disponible uniquement en anglais]
ETSI GS INS 002	[Disponible uniquement en anglais]
ETSI TR 102 764	[Disponible uniquement en anglais]
ETSI TR 103 370	[Disponible uniquement en anglais]
ETSI TR 103 644	[Disponible uniquement en anglais]
ETSI TR 103 591	[Disponible uniquement en anglais]
ETSI TS 133 501	[Disponible uniquement en anglais]
IEC 62443-4-2	Sécurité des systèmes d'automatisation et de commande industrielles – Partie 4-2 : Exigences de sécurité technique des composants IACS

IEC 61158-4-2	Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4- 2 : Spécification du protocole de la couche liaison de données – Éléments de type 2
IEC 61158-4-25	Réseaux de communication industriels – Spécifications des bus de terrain – Partie 4-25 : Spécification du protocole de la couche liaison de données – Eléments de type 25
IEC TS 63134	[Disponible uniquement en anglais]
IEEE 1888 SERIES	[Disponible uniquement en anglais]
IEEE 802.1AE	[Disponible uniquement en anglais]
IEEE 2410	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
IEEE 802.17	[Disponible uniquement en anglais]
IES LM-63	[Disponible uniquement en anglais]
ISO 11577	TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – PROTOCOLE DE SÉCURITÉ DE LA COUCHE RÉSEAU
ISO 18185-4	CONTENEURS POUR LE TRANSPORT DE MARCHANDISES – SCELLÉS ÉLECTRONIQUES – PARTIE 4 : PROTECTION DES DONNÉES
ISO 20215	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – ALGORITHMES CRYPTOGRAPHIQUES CCSDS
ISO 21091	INFORMATIQUE DE SANTÉ – SERVICES D'ANNUAIRES POUR LES FOURNISSEURS DE SOINS DE SANTÉ, LES SUJETS DE SOINS ET AUTRES ENTITÉS
ISO 21324	SYSTÈMES DE TRANSFERT DES DONNÉES ET INFORMATIONS SPATIALES – PROTOCOLE DE SÉCURITÉ DE LIAISON DE DONNÉES SPATIALES
ISO 21549-2	INFORMATIQUE DE SANTÉ – DONNÉES RELATIVES AUX CARTES DE SANTÉ DES PATIENTS – PARTIE 2 : OBJETS COMMUNS
ISO 21549-3	INFORMATIQUE DE SANTÉ – DONNÉES RELATIVES AUX CARTES DE SANTÉ DES PATIENTS – PARTIE 3 : DONNÉES CLINIQUES LIMITÉES
ISO 21549-4	INFORMATIQUE DE SANTÉ – DONNÉES RELATIVES AUX CARTES DE SANTÉ DES PATIENTS – PARTIE 4 : DONNÉES CLINIQUES ÉTENDUES
ISO 21549-5	INFORMATIQUE DE SANTÉ – DONNÉES RELATIVES AUX CARTES DE SANTÉ DES PATIENTS – PARTIE 5 : DONNÉES D'IDENTIFICATION
ISO 21549-6	INFORMATIQUE DE SANTÉ – DONNÉES RELATIVES AUX CARTES DE SANTÉ DES PATIENTS – PARTIE 6 : DONNÉES ADMINISTRATIVES
ISO 27799	INFORMATIQUE DE SANTÉ – MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION RELATIVE À LA SANTÉ EN UTILISANT L'ISO/IEC 27002
ISO/IEC 10116	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – MODES OPÉRATOIRES POUR UN CHIFFREMENT PAR BLOCS DE N BITS – AMENDEMENT 1
ISO/IEC 10181-5-00	TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS : CADRE DE CONFIDENTIALITÉ
ISO/IEC 11577-97	[Disponible uniquement en anglais]
ISO/IEC 19772	SÉCURITÉ DE L'INFORMATION – CHIFFREMENT AUTHENTIFIÉ
ISO/IEC 19794-11	TECHNOLOGIES DE L'INFORMATION – FORMATS D'ÉCHANGE DE DONNÉES BIOMÉTRIQUES – PARTIE 11 : DONNÉES DYNAMIQUES TRAITÉES DE SIGNATURE/SIGNE
ISO/IEC 19794-13	TECHNOLOGIES DE L'INFORMATION – FORMATS D'ÉCHANGES DE DONNÉES BIOMÉTRIQUES – PARTIE 13 : DONNÉES RELATIVES À LA VOIX
ISO/IEC 19794-7	TECHNOLOGIES DE L'INFORMATION – FORMATS D'ÉCHANGE DE DONNÉES BIOMÉTRIQUES – PARTIE 7 : DONNÉES DE SÉRIE CHRONOLOGIQUE DE SIGNATURE/SIGNE
ISO/IEC 24713-2	Technologies de l'information – Profils biométriques pour interopérabilité et échange de données – Partie 2 : Contrôle d'accès physique pour les employés aux aéroports
ISO/IEC 29150/	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SIGNCRYPTAGE

ISO/IEC 30107-2	TECHNOLOGIES DE L'INFORMATION – DÉTECTION D'ATTAQUE DE PRÉSENTATION EN BIOMÉTRIE – PARTIE 2 : FORMAT DES DONNÉES
ISO/IEC/IEEE 18883	Technologies de l'information – Protocole de contrôle de la communauté verte omniprésente – Sécurité
ISO 10781	INFORMATIQUE DE SANTÉ – MODÈLE FONCTIONNEL D'UN SYSTÈME DE DOSSIER DE SANTÉ INFORMATISÉ, PUBLICATION 2 (EHR FM)
ISO TS 27790	INFORMATIQUE DE SANTÉ – CADRE D'ENREGISTREMENT DE DOCUMENT
ISO 20078-3	VÉHICULE ROUTIERS – WEB SERVICES DU VÉHICULE ÉTENDU (EXVE) – PARTIE 3 : SÉCURITÉ
ISO TR 12859	SYSTÈMES INTELLIGENTS DE TRANSPORT – ARCHITECTURE DE SYSTÈME – ASPECTS PRIVÉS DANS LES NORMES ET LES SYSTÈMES SIT
ISO 12855	PERCEPTION DU TÉLÉPÉAGE – ÉCHANGE D'INFORMATIONS ENTRE LA PRESTATION DE SERVICE ET LA PERCEPTION DU PÉAGE
ISO 13399-1	REPRÉSENTATION ET ÉCHANGE DES DONNÉES RELATIVES AUX OUTILS COUPANTS – PARTIE 1 : VUE D'ENSEMBLE, PRINCIPES FONDAMENTAUX ET MODÈLE GÉNÉRAL D'INFORMATIONS
ISO 18440	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – EXTENSION DE LIAISONS SPATIALES – PROTOCOLE INTERNET POUR SERVICES DE TRANSFERT
ISO 19115-1	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ISO 20208	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – FORMAT D'ÉCHANGE DES DONNÉES BRUTES DELTA-DOR
ISO 21076	DONNÉES SPATIALES ET SYSTÈMES DE TRANSFERT D'INFORMATION – SUPPORT CROISÉ DES COMMUNICATIONS SPATIALES – EXIGENCES D'ARCHITECTURE
ISO 22663	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – PROTOCOLE POUR LIAISONS SPATIALES DE PROXIMITÉ 1 – COUCHE DE LIAISONS DE DONNÉES
ISO/IEC 17417	TECHNOLOGIES DE L'INFORMATION – TÉLÉINFORMATIQUE – COMMUNICATION À COURTE DISTANCE UTILISANT LA LUMIÈRE VISIBLE (SDVLC)
ISO/IEC 20248	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES D'IDENTIFICATION AUTOMATIQUE ET DE CAPTURE DE DONNÉES – STRUCTURES DE DONNÉES – MÉTA-STRUCTURE DE SIGNATURE NUMÉRIQUE
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO TS 22220	INFORMATIQUE DE SANTÉ – IDENTIFICATION DES SUJETS DE SOINS SANITAIRES
ISO/IEC 13871-97	[Disponible uniquement en anglais]
ISO/IEC 9798-6	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – AUTHENTIFICATION D'ENTITÉ – PARTIE 6 : MÉCANISMES UTILISANT UN TRANSFERT MANUEL DE DONNÉES
ISO/TS 22220	Informatique de santé – Identification des sujets de soins sanitaires
ISO/IEC/IEEE 8802-3	Télécommunications et échange entre systèmes informatiques – Exigences pour les réseaux locaux et métropolitains – Partie 3 : Norme pour Ethernet
ISO 15396	SYSTÈMES DE TRANSFERT DES DONNÉES ET INFORMATIONS SPATIALES – MODÈLE DE RÉFÉRENCE POUR LE SUPPORT CROISÉ – SERVICES D'EXTENSION DE LIAISONS SPATIALES
ISO 18750	SYSTÈME DE TRANSPORTS INTELLIGENTS – SYSTÈMES COOPÉRATIFS – CARTE LOCALE DYNAMIQUE
ISO 23354	TITRE MANQUE
ISO/IEC 24761:20	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CONTEXTE D'AUTHENTIFICATION BIOMÉTRIQUE
ISO/IEC TR 30164	L'INTERNET DES OBJETS (IOT) – INFORMATIQUE EN PÉRIPHÉRIE
ISO/TR 23786	VÉHICULES ROUTIERS – SOLUTIONS RELATIVES À L'ACCÈS À DISTANCE DU VÉHICULE – CRITÈRES D'ÉVALUATION DES RISQUES
ISO/TR 23791	Véhicules routiers – Web services du véhicule étendu (ExVe) – Résultats de l'évaluation des risques de la série de normes ISO 20078
ISO/TS 18750	Système de transports intelligents – Systèmes coopératifs – Carte locale dynamique

ISO/IEC 27034-6	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DES APPLICATIONS – PARTIE 6 : ÉTUDES DE CAS
ISO 22857	INFORMATIQUE DE SANTÉ – LIGNES DIRECTRICES SUR LA PROTECTION DES DONNÉES POUR FACILITER LES FLUX D'INFORMATION SUR LA SANTÉ DU PERSONNEL DE PART ET D'AUTRE DES FRONTIÈRES
ISO/IEC 15944-12	TECHNOLOGIES DE L'INFORMATION – VUE OPÉRATIONNELLE D'AFFAIRES – PARTIE 12 : EXIGENCES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE (PPR) RELATIVES À LA GESTION DU CYCLE DE VIE DE L'INFORMATION (ILCM) ET DE L'EDI DES RENSEIGNEMENTS PERSONNELS (PI)
ISO TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO/IEC TR 23186	[Disponible uniquement en anglais]
ISO/TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO/IEC TR 27550	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – INGÉNIERIE DE LA VIE PRIVÉE POUR LES PROCESSUS DU CYCLE DE VIE DES SYSTÈMES
ITU-T G.9961	Émetteurs-récepteurs de réseau domestique filaires unifiés à haut débit – Couche de liaison de données
ITU-T Y.4468	Protocole de transfert de l'ensemble minimal de données pour le système d'intervention d'urgence pour automobile
ITU-T Q.1229	Guide d'utilisation du réseau intelligent pour l'ensemble de capacités 2
ITU-T Y.3509	Informatique en nuage – Architecture fonctionnelle pour la fédération du stockage des données
ITU-T SERIES Q SUPP 30	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 30	[Disponible uniquement en anglais]
ITU-T X.1642	[Disponible uniquement en anglais]
ITU-T Y.1311.1	Réseau privé virtuel IP sur réseau utilisant l'architecture MPLS
ITU-T Y.3600	Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage
SAE AIR6904	[Disponible uniquement en anglais]
SAE ARP4294	[Disponible uniquement en anglais]
SAE GEIA-HB-0007-B	[Disponible uniquement en anglais]
UL 2196	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
IEEE P7002	[Disponible uniquement en anglais]
DIACC PCTF 04	Cadre de confiance pancanadien Respect de la vie privée : Aperçu et Profil de conformité
DIACC PCTF 02	Cadre de confiance pancanadien Avis et consentement : Aperçu et Profil de conformité
CAN/CIOSC 104	Contrôles de cybersécurité de base pour les petites et moyennes organisations
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données

CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 109-2	Cadre canadien de protection de la confidentialité des informations
CAN/CIOSC 109-1	Qualification et maîtrise des professionnels de la confidentialité et du contrôle d'accès
ISO/IEC 27400	[Disponible uniquement en anglais]
ISO/IEC 27402	[Disponible uniquement en anglais]
ISO/IEC 27403	[Disponible uniquement en anglais]
CSA T100**	Code du bâtiment : technologies de l'information et de la communication
CSA T200**	Programme de développement de logiciels et d'évaluation de la cybersécurité
CSA EXP 200	[Disponible uniquement en anglais]
CSA T2000-1**	[Disponible uniquement en anglais]
CSA T2000-2**	Système intelligent de gestion de la sécurité du système du bâtiment
CSA Z246.1	Gestion de la sûreté des installations liées à l'industrie du pétrole et du gaz naturel – quatrième édition
CSA T150**	Code du véhicule connecté et automatisé (CAV)
CSA T710**	Méthodologie et exigences d'évaluation de la préparation à la fabrication intelligente
CAN/CSA-ISO 14971	Dispositifs médicaux – Application de la gestion des risques aux dispositifs médicaux
CAN/CSA-CEI/IEC 62304	Logiciels de dispositifs médicaux – Processus du cycle de vie du logiciel

Question clé 7
des conseils sur la fiabilité, l'utilisation éthique et sociétale des données

ISO/IEC 38505.2	[Disponible uniquement en anglais]
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO 10711	Systèmes intelligents de transport – Protocole d'interface et définition des ensembles de messages entre régulateurs de signaux de circulation et détecteurs
ISO 12655	Performance énergétique des bâtiments – Présentation de l'utilisation énergétique réelle des bâtiments
ISO 13790	Performance énergétique des bâtiments – Calcul des besoins d'énergie pour le chauffage et le refroidissement des locaux
ISO TR 17755	Sécurité incendie – Aperçu général sur les pratiques nationales de collecte des statistiques d'incendies
ISO TS 14048	Management environnemental – Analyse du cycle de vie – Format de documentation de données
ISO/IEC 19795-1	Technologies de l'information – Essais et rapports de performance
ISO/IEC 29155-1	Ingénierie des systèmes et du logiciel – Cadre de conduite de tests de performance de projet de technologies de l'information – Partie 1 : Concepts et définitions
ISO/IEC 29155-4	Ingénierie des systèmes et du logiciel – Cadre de conduite de tests de performance de projet de technologies de l'information – Partie 4 : Directives pour la collecte de données et la maintenance
ISO/TS 14048	Management environnemental – Analyse du cycle de vie – Format de documentation de données
ASTM E2129	[Disponible uniquement en anglais]
ASTM E2166	[Disponible uniquement en anglais]

ASTM E2797	[Disponible uniquement en anglais]
DIN SPEC 91367	[Disponible uniquement en anglais]
ETSI GS OSG 001	[Disponible uniquement en anglais]
IEEE 1616	[Disponible uniquement en anglais]
IEEE 1856	[Disponible uniquement en anglais]
ITU-R RS.1859	[Disponible uniquement en anglais]
ITU-R SA.1164-4	[Disponible uniquement en anglais]
ITU-R SA.1627	[Disponible uniquement en anglais]
ITU-T X.1603	[Disponible uniquement en anglais]
ITU-T Y.3603	Mégadonnées – Exigences et modèle conceptuel applicables aux métadonnées pour les catalogues de données
BSI BS 10102-1	[Disponible uniquement en anglais]
CEN 16234-1	Référentiels de e-Compétences – Référentiel européen commun pour les professionnels des technologies de l'information et de la communication dans tous les secteurs – Partie 1 : Référentiel
CEN 17161	Conception pour tous – Accessibilité suivant une approche de la « Conception pour tous » des produits, des biens et des services – Élargissement de l'éventail d'utilisateurs
ISO 26000	LIGNES DIRECTRICES RELATIVES À LA RESPONSABILITÉ SOCIÉTALE
ISO/IEC TR 29196	Technologies de l'information – Directives pour l'inscription biométrique
ISO/IEC/IEEE 24765	Ingénierie des systèmes et du logiciel – Vocabulaire
ISO/TR 14639-2	Informatique de santé – Feuille de route de l'architecture de santé électronique fondée sur la capacité – Partie 2 : Composants architecturaux et modèle de maturité
ISO/TR 16982	ERGONOMIE DE L'INTERACTION HOMME-SYSTÈME – MÉTHODES D'UTILISABILITÉ POUR LA CONCEPTION CENTRÉE SUR L'OPÉRATEUR HUMAIN
ISO/TR 18638	INFORMATIQUE DE SANTÉ – COMPOSANTES ÉDUCATIVES DESTINÉES À GARANTIR LA CONFIDENTIALITÉ DES INFORMATIONS RELATIVES À LA SANTÉ
ISO/TR 21548	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Lignes directrices
ISO/TR 22221	Informatique de santé – Principes et indications d'exploitation d'un entrepôt de données cliniques
ISO/TR 22758	BIOTECHNOLOGIE – BIOBANKING – GUIDE DE MISE EN OEUVRE DE L'ISO 20387
ISO/TS 14265	Informatique de santé – Classification des besoins pour le traitement des informations de santé personnelles
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO/TS 22220	Informatique de santé – Identification des sujets de soins sanitaires
IEEE 7010	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données
DS DS/CWA 17145-1	[Disponible uniquement en anglais]
GOST K32095	[Disponible uniquement en anglais]
CLSI I/LA21-A2	[Disponible uniquement en anglais]
BSI BS 42020	[Disponible uniquement en anglais]
BSI PAS 183	[Disponible uniquement en anglais]
BSI PAS 185	[Disponible uniquement en anglais]
CSA PLUS 8300-96	[Disponible uniquement en anglais]
CLSI H26-A2	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 45	[Disponible uniquement en anglais]

DS DS-håndbog 107.2	[Disponible uniquement en anglais]
CEN/TR 15592	Services en santé – Systèmes de management de la qualité – Guide d'utilisation de l'EN ISO 9004:2000 pour l'amélioration continue des performances dans les services en santé
ISO/IEC 38505-1	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 101:2019	Intelligence artificielle : Conception éthique et utilisation de systèmes de décision automatisés
IEEE 7000 Series	[Disponible uniquement en anglais]
IEEE P2840	[Disponible uniquement en anglais]

Question clé 8
harmonisation et interprétabilité des pratiques de données/données ouvertes

ISO 5479	INTERPRÉTATION STATISTIQUE DES DONNÉES – TESTS POUR LES ÉCARTS À LA DISTRIBUTION NORMALE
ISO/IEC 9646-3	TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS – ESSAIS DE CONFORMITÉ – MÉTHODOLOGIE GÉNÉRALE ET PROCÉDURES – PARTIE 3 : NOTATION COMBINÉE, ARBORESCENTE ET TABULAIRE (TTCN)
ISO/IEC TR 10171	Technologies de l'information – Télécommunications et échange d'information entre systèmes – Liste de protocoles normalisés pour la couche liaison de données employant des classes de procédures de commande de liaison de données à haut niveau (HDLC) et liste d'identificateurs normalisés de format XID, liste d'identificateurs normalisés de format du champ d'information sur la programmation de mode et liste des valeurs d'identification pour les jeux de paramètres normalisés définis par les utilisateurs
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO/IEC 20016-1	TECHNOLOGIES DE L'INFORMATION POUR L'APPRENTISSAGE, L'ÉDUCATION ET LA FORMATION – ACCESSIBILITÉ AU LANGAGE ET ÉQUIVALENCES D'INTERFACE HUMAINES (HIES) DANS LES APPLICATION D'APPRENTISSAGE ÉLECTRONIQUE – PARTIE 1 : CADRE ET MODÈLE DE RÉFÉRENCE POUR L'INTEROPÉRABILITÉ SÉMANTIQUE
ITU-T H.812	Directives de conception visant à assurer l'interopérabilité des systèmes de santé individuels : Interface de service : Classe de dispositifs certifiés commune
ITU-T H.830.1	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 1 : Interopérabilité des services web : Émetteur de services de santé et de forme physique
ITU-T H.830.10	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 10 : Chargement des observations hData : Récepteur de services de santé et de forme physique
ITU-T H.830.11	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 11 : Questionnaires : Émetteur de services de santé et de forme physique

ITU-T H.830.12	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 12 : Questionnaires : Récepteur de services de santé et de forme physique
ITU-T H.830.13	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 13 : Échange de capacités : Émetteur de services de santé et de forme physique
ITU-T H.830.14	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 14 : Échange de capacités : Récepteur de services de santé et de forme physique
ITU-T H.830.15	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 15 : Chargement des observations FHIR : Émetteur de services de santé et de forme physique
ITU-T H.830.16	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 16 : Chargement des observations FHIR : Récepteur de services de santé et de forme physique
ITU-T H.830.2	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 2 : Interopérabilité des services web : Récepteur de services de santé et de forme physique
ITU-T H.830.4	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 4 : SOAP/ATNA : Récepteur de services de santé et de forme physique
ITU-T H.830.5	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 5 : Messages PCD-01 HL7 : Émetteur de services de santé et de forme physique
ITU-T H.830.7	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 7 : Gestion des consentements : Émetteur de services de santé et de forme physique
ITU-T H.830.8	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 8 : Gestion des consentements : Récepteur de services de santé et de forme physique
ITU-T H.830.9	Conformité des systèmes individuels de suivi de l'état de santé UIT-T H.810 : Interface pour les services – Partie 9 : Chargement des observations hData : Émetteur de services de santé et de forme physique
ITU-T H.831	Conformité des dispositifs individuels de suivi de l'état de santé UIT-T H.810 : Interface WAN – Partie 1 : Interopérabilité des services web : Émetteur
ITU-T H.832	Conformité des dispositifs individuels de suivi de l'état de santé UIT-T H.810 : Interface WAN – Partie 2 : Interopérabilité des services web : Récepteur
ITU-T H.834	Conformité des dispositifs individuels de suivi de l'état de santé UIT-T H.810 : Interface WAN – Partie 4 : SOAP/ATNA : Récepteur
ITU-T H.835	Conformité des dispositifs individuels de suivi de l'état de santé UIT-T H.810 : Interface WAN – Partie 5 : Messages PCD-01 HL7 : Émetteur
ITU-T H.836	Conformité des dispositifs individuels de suivi de l'état de santé UIT-T H.810 : Interface WAN – Partie 6 : Messages PCD-01 HL7 : Récepteur
ITU-T H.837	Conformité des dispositifs individuels de suivi de l'état de santé UIT-T H.810 : Interface WAN – Partie 7 : Gestion des consentements : Émetteur
ITU-T H.838	Conformité des dispositifs individuels de suivi de l'état de santé UIT-T H.810 : Interface WAN – Partie 8 : Gestion des consentements : Récepteur
ITU-T Q.3954	oneM2M – Tests d'interopérabilité
ISO 8000-61	Qualité des données – Partie 61 : Gestion de la qualité des données : Modèle de référence des procédés
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 38505-1	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC TR 38502	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TI – CADRE GÉNÉRAL ET MODÈLE

ISO/IEC TR 38504	GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – LIGNES DIRECTRICES POUR DES NORMES FONDÉES SUR DES PRINCIPES RELATIVES À LA GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION
ISO/IEC TS 38501	Technologies de l'information – Gouvernance des technologies de l'information – Guide d'implémentation
SNZ AS/NZS 8016	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO/IEC 27560	[Disponible uniquement en anglais]
ISO/IEC 38505-1:2017	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données
N/A	[Disponible uniquement en anglais]
N/A	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 103-4	Confiance et identité numérique – Partie 4 : Portefeuilles numériques
IEEE 1900.6-2011	[Disponible uniquement en anglais]
IEEE P2896	[Disponible uniquement en anglais]
IEEE P1484.11.1	[Disponible uniquement en anglais]
IEEE 1609.11-2010	[Disponible uniquement en anglais]
IEEE C37.118.2-2011	[Disponible uniquement en anglais]
IEEE/IEC C37.111-2013	[Disponible uniquement en anglais]
IEEE 1451.0-2007	[Disponible uniquement en anglais]
IEEE 2418.2-2020	[Disponible uniquement en anglais]
n/a	Statistique Canada Normes statistiques (Concepts, classifications et variables)
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]

Question clé 9
rôles d'acteur du traitement des données et de transaction de données

CEN EN 13608-3	[Disponible uniquement en anglais]
SNZ AS/NZS 5478	[Disponible uniquement en anglais]
CEN/TR 15449-3	Information géographique – Infrastructures de données spatiales – Partie 3 : vue centrée sur les données d'une infrastructure de données spatiales (IDS)
ITU-T X.1603	[Disponible uniquement en anglais]
ITU-T X.1641	[Disponible uniquement en anglais]
ISO 16175.1	INFORMATION ET DOCUMENTATION – PROCESSUS ET EXIGENCES FONCTIONNELLES APPLICABLES AUX LOGICIELS DE GESTION DES DOCUMENTS D'ACTIVITÉ – PARTIE 1 : EXIGENCES FONCTIONNELLES ET RECOMMANDATIONS ASSOCIÉES POUR TOUTE APPLICATION DE GESTION DE DOCUMENTS D'ACTIVITÉ NUMÉRIQUES

ISO 16175-1	INFORMATION ET DOCUMENTATION – PROCESSUS ET EXIGENCES FONCTIONNELLES APPLICABLES AUX LOGICIELS DE GESTION DES DOCUMENTS D'ACTIVITÉ – PARTIE 1 : EXIGENCES FONCTIONNELLES ET RECOMMANDATIONS ASSOCIÉES POUR TOUTE APPLICATION DE GESTION DE DOCUMENTS D'ACTIVITÉ NUMÉRIQUES
ASTM D4840	[Disponible uniquement en anglais]
ASTM E2147	[Disponible uniquement en anglais]
ETSI TS 187 001	[Disponible uniquement en anglais]
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO 8000-61	Qualité des données – Partie 61 : Gestion de la qualité des données : Modèle de référence des procédés
ISO TS 8000-150	QUALITÉ DES DONNÉES – PARTIE 150 : DONNÉES PERMANENTES : CADRE DE MANAGEMENT DE LA QUALITÉ
ISO/TS 8000-150	Qualité des données – Partie 150 : Données permanentes : Cadre de management de la qualité
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
N/A	Lignes directrices du CEPD sur les notions de responsable du traitement, de sous-traitant et de responsabilité conjointe du traitement dans le cadre du règlement (UE) 2018/1725
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 109-2	[Disponible uniquement en anglais]
IEEE 117-2015	[Disponible uniquement en anglais]
IEEE P2957	[Disponible uniquement en anglais]
IEEE P802.3cy	[Disponible uniquement en anglais]
IEEE 1588-2019	[Disponible uniquement en anglais]
IEEE P2144.2	[Disponible uniquement en anglais]
IEEE P802.1CBcv	[Disponible uniquement en anglais]
IEEE P2418.2	[Disponible uniquement en anglais]

Question clé 10
réutilisation des données

DS DS/CWA 17145-1	[Disponible uniquement en anglais]
ISO/IEC 29184	TECHNOLOGIES DE L'INFORMATION – DÉCLARATIONS DE CONFIDENTIALITÉ EN LIGNE ET LES CONSENTEMENTS
ISO/IEC 24760-2	Technologies de l'information – Techniques de sécurité – cadre pour la gestion de l'identité – Partie 2 : Architecture de référence et exigences
CSA CSA-Q830-03	Code type sur la protection des renseignements personnels

CSA PLUS 8300-96	[Disponible uniquement en anglais]
DS DS/CWA 14355	[Disponible uniquement en anglais]
ETSI TR 102 458	[Disponible uniquement en anglais]
ETSI TR 103 534-2	[Disponible uniquement en anglais]
IEC 61970-405	[Disponible uniquement en anglais]
IEC 62541-8	Architecture unifiée OPC – Partie 8 : Accès aux données
ISO 19115.1	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ISO 19115-1	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ISO 19132	INFORMATION GÉOGRAPHIQUE – SERVICES BASÉS SUR LA LOCALISATION – MODÈLE DE RÉFÉRENCE
ISO/IEC 7816-11	CARTES D'IDENTIFICATION – CARTES À CIRCUIT INTÉGRÉ – PARTIE 11 : VERIFICATION PERSONELLE PAR MÉTHODES BIOMÉTRIQUES
ISO/IEC TR 24729-4	TECHNOLOGIES DE L'INFORMATION – IDENTIFICATION DE RADIOFRÉQUENCES POUR LA GESTION D'ITEMS – LIGNES DIRECTRICES POUR LA MISE EN OEUVRE – PARTIE 4 : SÉCURITÉ DES DONNÉES DE REPÈRE
ISO/IEC 24791-5	TECHNOLOGIES DE L'INFORMATION – IDENTIFICATION DE RADIOFR ÉQUENCE (RFID) POUR LA GESTION D'ÉLÉMENT – INFRASTRUCTURE DE SYSTÈMES LOGICIELS – PARTIE 5 : INTERFACE DE DISPOSITIF
ISO/IEC 9579-04	Technologies de l'information – Accès à la base de données à distance pour SQL avec sécurité accrue
ANSI INCITS 504-1	[Disponible uniquement en anglais]
ETSI TS 102 342	[Disponible uniquement en anglais]
ETSI TS 103 458	[Disponible uniquement en anglais]
ETSI TS 103 532	[Disponible uniquement en anglais]
ETSI TS 183 064	[Disponible uniquement en anglais]
IEEE 1619.2	[Disponible uniquement en anglais]
IEC 62628	Lignes directrices concernant la sûreté de fonctionnement du logiciel
ISO/IEC 30182	MODÈLE DE CONCEPT DE VILLE INTELLIGENTE – LIGNES DIRECTRICES POUR ÉTABLIR UN MODÈLE D'INTEROPÉRABILITÉ DES DONNÉES
ISO/IEC 25024	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – EXIGENCES ET ÉVALUATION DE LA QUALITÉ DES SYSTÈMES ET DU LOGICIEL (SQUARE) – MESURAGE DE LA QUALITÉ DES DONNÉES
IEEE 1232.1	[Disponible uniquement en anglais]
IEEE STDVA24228	[Disponible uniquement en anglais]
ITU-T X.1602	[Disponible uniquement en anglais]
ITU-T Y.3602	Mégadonnées – Exigences fonctionnelles relatives à la provenance des données
ISO/IEC TR 20547-2	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 2 : CAS PRATIQUES ET EXIGENCES DÉRIVÉES
ISO/IEC TR 23186	[Disponible uniquement en anglais]
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO/IEC 38505.2	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – PARTIE 2 : IMPLICATIONS DE L'ISO/IEC 38505-1 POUR LA GESTION DES DONNÉES
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC 22624	[Disponible uniquement en anglais]

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO/IEC TS 19249	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CATALOGUE DES PRINCIPES ARCHITECTURAUX ET CONCEPTUELS POUR LA SÉCURISATION DES PRODUITS, SYSTÈMES ET APPLICATIONS
ISO/IEC 23751	[Disponible uniquement en anglais]
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO 22624	[Disponible uniquement en anglais]
ISO 26000	LIGNES DIRECTRICES RELATIVES À LA RESPONSABILITÉ SOCIÉTALE
IWA 26:2017	UTILISATION DE LA NORME ISO 26000:2010 DANS LES SYSTÈMES DE MANAGEMENT
IWA 27 – sharing economy (TC 324)	Principes directeurs et cadre de travail pour l'économie du partage
ISO/AWI 31700	[Disponible uniquement en anglais]
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 103-1:2020	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
CAN/CIOSC 109-2	Cadre canadien de protection de la confidentialité des informations
IEEE P2933	[Disponible uniquement en anglais]
IEEE P2876	[Disponible uniquement en anglais]
IEEE P7002	[Disponible uniquement en anglais]
IEEE P7012	[Disponible uniquement en anglais]
IEEE 2410	[Disponible uniquement en anglais]
DIACC PCTF 02	Cadre de confiance pancanadien Avis et consentement : Aperçu et Profil de conformité

Groupe de travail 2 : Collecte, organisation et classement

Question clé 11 collecte de données

BSI BS 17898	[Disponible uniquement en anglais]
DS DS/CWA 16385	[Disponible uniquement en anglais]
ETSI TS 103 458	[Disponible uniquement en anglais]
ISO 8000-61	Qualité des données – Partie 61 : Gestion de la qualité des données : Modèle de référence des procédés
ISO/IEC 12034-1	TECHNOLOGIES DE L'INFORMATION – ARCHIVE EXCHANGE FORMAT (AXF) – PARTIE 1 : STRUCTURE ET SÉMANTIQUE

ISO/IEC 12785-2	TECHNOLOGIES DE L'INFORMATION – APPRENTISSAGE, ÉDUCATION ET FORMATION – PAQUETAGE DU CONTENU – PARTIE 2 : LIAISON XML
ISO/IEC 23006-4	TECHNOLOGIES DE L'INFORMATION – TECHNOLOGIES DE LA PLATE-FORME DE SERVICES MULTIMÉDIA – PARTIE 4 : SERVICES ÉLÉMENTAIRES
ISO/IEC 29161	TECHNOLOGIES DE L'INFORMATION – STRUCTURE DE DONNÉES – IDENTIFICATION UNIQUE POUR L'INTERNET DES OBJETS
ISO/TS 14048	Management environnemental – Analyse du cycle de vie – Format de documentation de données
ITU-R SA.1627	Besoins de télécommunication et caractéristiques des systèmes de collecte de données et de localisation de plates-formes utilisés par les services SETS et MetSat
ITU-T SERIES Y SUPP 40	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 48	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 50	[Disponible uniquement en anglais]
ITU-T Y.2068	[Disponible uniquement en anglais]
ITU-T Y.2618	Interface M dans les réseaux publics de télécommunication pour les données en mode paquet
ITU-T Y.2619	Fonctions et mécanismes d'exploitation, d'administration et de maintenance pour le réseau public de télécommunication pour les données en mode paquets (PTDN)
ITU-T Y.2620	Interface T du réseau public de télécommunication pour les données en mode paquet
ITU-T Y.3071	Réseaux prenant en compte les données (réseaux centrés sur l'information) – Exigences et capacités
ITU-T Y.3174	Cadre pour le traitement des données en vue de permettre la mise en œuvre de l'apprentissage automatique dans les réseaux futurs, y compris les IMT-2020
ITU-T Y.3505	Informatique en nuage – Aperçu et exigences fonctionnelles pour la fédération du stockage des données
ITU-T Y.3518	Informatique en nuage – Exigences fonctionnelles de la gestion de données inter-nuages
ITU-T Y.3519	Informatique en nuage – Architecture fonctionnelle des mégadonnées en tant que service
ITU-T Y.3601	Mégadonnées – Cadre et exigences pour l'échange de données
ITU-T Y.3602	Mégadonnées – Exigences fonctionnelles relatives à la provenance des données
ITU-T Y.3603	Mégadonnées – Exigences et modèle conceptuel applicables aux métadonnées pour les catalogues de données
ITU-T Y.3604	Mégadonnées – Aperçu de la préservation des données et exigences
ITU-T Y.3650	Cadre applicable aux réseaux fondés sur les mégadonnées
ITU-T Y.3651	Gestion et planification du trafic dans les réseaux mobiles fondés sur les mégadonnées
ITU-T Y.4461	Cadre de données ouvertes dans les villes intelligentes
ITU-T Y.4467	Structure de l'ensemble minimal de données pour le système d'intervention d'urgence pour automobile
ITU-T Y.4468	Protocole de transfert de l'ensemble minimal de données pour le système d'intervention d'urgence pour automobile
NSC 120810000	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité

CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CSA Z8003	Recherche et évaluation de la conception des établissements de soins de santé

Question clé 12
gestion des systèmes de données

ASTM E2842	[Disponible uniquement en anglais]
DIN SPEC 4997	[Disponible uniquement en anglais]
ETSI GS ZSM 002	[Disponible uniquement en anglais]
IEC 62974-1	Systèmes de surveillance et de mesure utilisés pour la collecte et l'analyse de données – Partie 1 : Exigences relatives aux dispositifs
ISO 26162	Systèmes de gestion de la terminologie, de la connaissance et du contenu – Conception, mise en oeuvre et maintenance des systèmes de gestion de la terminologie
ISO 37156	INFRASTRUCTURES URBAINES INTELLIGENTES – CADRE DIRECTEUR POUR L'ÉCHANGE ET LE PARTAGE DE DONNÉES POUR LES INFRASTRUCTURES URBAINES INTELLIGENTES
ISO 8000-61	Qualité des données – Partie 61 : Gestion de la qualité des données : Modèle de référence des procédés
ISO/IEC 10164-1	Technologies de l'information – Interconnexion de systèmes ouverts (OSI)— Gestion-systèmes : Fonction de gestion d'objets – Amendement : 5/15/1996; Errata : 12/15/1996
ISO/IEC 10164-2	Technologies de l'information – Interconnexion de systèmes ouverts (OSI) – Gestion-systèmes : Fonction de gestion d'états – Amendement 1 : Formulaires de déclaration de conformité d'instance
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 27034-3	Technologie de l'information – Sécurité des applications – Partie 3 : Processus de gestion de la sécurité d'une application
ISO/IEC 29155-4	Ingénierie des systèmes et du logiciel – Cadre de conduite de tests de performance de projet de technologies de l'information – Partie 4 : Directives pour la collecte de données et la maintenance
ISO/IEC TR 10032	Technologies de l'information – Modèle de référence pour la gestion de données
ISO/IEC TR 30164	L'internet des objets (IoT) – Informatique en périphérie
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ITU-T M.3041	Cadre pour l'exploitation, la gestion et la maintenance intelligentes
ITU-T M.3363	Exigences pour la gestion des données dans le réseau de gestion des télécommunications
ITU-T Y.3518	Informatique en nuage – Exigences fonctionnelles de la gestion de données inter-nuages
ITU-T Y.3604	Mégadonnées – Aperçu de la préservation des données et exigences
SAE GEIA-859A	[Disponible uniquement en anglais]
SAE GEIA-HB-859	[Disponible uniquement en anglais]

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données

Question clé 13
découvrabilité des données

ANSI INCITS 284	[Disponible uniquement en anglais]
ANSI INCITS 504-1	[Disponible uniquement en anglais]
ETSI TS 103 532	[Disponible uniquement en anglais]
IEC 62541-8	Architecture unifiée OPC – Partie 8 : Accès aux données
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 24091	[Disponible uniquement en anglais]
ISO/IEC 7816-11	CARTES D'IDENTIFICATION – CARTES À CIRCUIT INTÉGRÉ – PARTIE 11 : VERIFICATION PERSONELLE PAR MÉTHODES BIOMÉTRIQUES
ISO/IEC 9579-04	Technologies de l'information – Accès à la base de données à distance pour SQL avec sécurité accrue
ISO/TR 17424	Systèmes intelligents de transport – Systèmes coopératifs – État des connaissances des cartes dynamiques locales
ISO 19115.1	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ETSI TS 103 458	[Disponible uniquement en anglais]
IEC TS 61850-7-7	[Disponible uniquement en anglais]
ISO/IEEE 11073-10101	Informatique de santé – Interopérabilité des dispositifs – Partie 10101 : Communication entre dispositifs médicaux sur le site des soins – Nomenclature
CLSI AUTO16	[Disponible uniquement en anglais]
DIN SPEC 91357	[Disponible uniquement en anglais]
ISO 20078-3	VÉHICULE ROUTIERS – WEB SERVICES DU VÉHICULE ÉTENDU (EXVE) – PARTIE 3 : SÉCURITÉ
BSI BS 10012 + A1	[Disponible uniquement en anglais]
CEN EN 16931-1	Facturation électronique – Partie 1 : Modèle sémantique de données des éléments essentiels d'une facture électronique
DIN CEN/TS 17262	Identification personnelle – Recommandations pour garantir la robustesse de la biométrie dans les systèmes de contrôle frontalier automatisés européens contre les attaques de présentation
DS DS/CEN/TR 16931-4	[Disponible uniquement en anglais]
DS DS/CEN/TS 17262	[Disponible uniquement en anglais]
ETSI EN 300 175-4	[Disponible uniquement en anglais]
ETSI TR 103 305-5	[Disponible uniquement en anglais]
ETSI TR 103 370	[Disponible uniquement en anglais]
ETSI TR 103 591	[Disponible uniquement en anglais]
ETSI TS 102 563	[Disponible uniquement en anglais]
ETSI TS 103 466	[Disponible uniquement en anglais]
ISO 17427-1	SYSTÈMES DE TRANSPORT INTELLIGENTS – SYSTÈMES DE TRANSPORT COOPÉRATIFS INTELLIGENTS – PARTIE 1 : RÔLES ET RESPONSABILITÉS DANS LE CONTEXTE DES STI FONDÉS SUR L'ARCHITECTURE
ISO 17892-12	RECONNAISSANCE ET ESSAIS GÉOTECHNIQUES – ESSAIS DE LABORATOIRE SUR LES SOLS – PARTIE 12 : DÉTERMINATION DES LIMITES DE LIQUIDITÉ ET DE PLASTICITÉ
ISO 18185-4	CONTENEURS POUR LE TRANSPORT DE MARCHANDISES – SCELLÉS ÉLECTRONIQUES – PARTIE 4 : PROTECTION DES DONNÉES
ISO 24534-3	SYSTÈMES DE TRANSPORT INTELLIGENTS – IDENTIFICATION AUTOMATIQUE DES VÉHICULES ET DES ÉQUIPEMENTS – IDENTIFICATION D'ENREGISTREMENT ÉLECTRONIQUE (ERI) POUR LES VÉHICULES – PARTIE 3 : DONNÉES DU VÉHICULE

ISO 13527	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – STRUCTURE DES UNITÉS DE DONNÉES FORMATÉES XML (XFDU) ET RÈGLES DE CONSTRUCTION
ISO 14199	INFORMATIQUE DE SANTÉ – MODÈLE D'INFORMATION – MODÈLE DE GROUPE DE DOMAINE INTÉGRÉ DE RECHERCHE BIOMÉDICALE (BRIDG)
ISO 14825	SYSTÈMES INTELLIGENTS DE TRANSPORT – FICHIERS DE DONNÉES GÉOGRAPHIQUES (GDF) – GDF5.0
ISO 15489-1	INFORMATION ET DOCUMENTATION – GESTION DES DOCUMENTS D'ACTIVITÉ – PARTIE 1 : CONCEPTS ET PRINCIPES
ISO 15836-1	INFORMATION ET DOCUMENTATION – L'ENSEMBLE DES ÉLÉMENTS DE MÉTADONNÉES DUBLIN CORE – PARTIE 1 : ÉLÉMENTS PRINCIPAUX
ISO 15836-2	INFORMATION ET DOCUMENTATION – L'ENSEMBLE DES ÉLÉMENTS DE MÉTADONNÉES DUBLIN CORE – PARTIE 2 : TITRE MANQUE
ISO 16684-1	TECHNOLOGIE GRAPHIQUE – SPÉCIFICATION DE LA PLATE-FORME DE MÉTADONNÉES EXTENSIBLES (XMP) – PARTIE 1 : MODÈLE DE DONNÉES, MISE EN SÉRIE ET PARAMÈTRES PRINCIPAUX
ISO 16684-2	TECHNOLOGIE GRAPHIQUE – PLATE-FORME DE MÉTADONNÉES EXTENSIBLES (XMP) – PARTIE 2 : DESCRIPTION DES SCHÉMAS XMP UTILISANT RELAX NG
ISO 17316	INFORMATION ET DOCUMENTATION – IDENTIFICATION DE CONNEXION STANDARD INTERNATIONAL (ISLI)
ISO 17972-1	TECHNOLOGIE GRAPHIQUE – FORMAT D'ÉCHANGE DES DONNÉES EN COULEUR – PARTIE 1 : RELATION AVEC LE CXF3 (CXF/X)
ISO 17972-2	TECHNOLOGIE GRAPHIQUE – ÉCHANGE DES DONNÉES DE COULEUR EN UTILISANT CXF – PARTIE 2 : DONNÉES CIBLES DU SCANNER ENTRANTES
ISO 17972-3	TECHNOLOGIE GRAPHIQUE – ÉCHANGE DES DONNÉES DE COULEUR EN UTILISANT CXF – PARTIE 3 : DONNÉES CIBLES SORTANTES
ISO 19109	INFORMATION GÉOGRAPHIQUE – RÈGLES DE SCHÉMA D'APPLICATION
ISO 19111	INFORMATION GÉOGRAPHIQUE – SYSTÈME DE RÉFÉRENCES PAR COORDONNÉES
ISO 19115.2	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 2 : EXTENSIONS POUR L'ACQUISITION ET LE TRAITEMENT
ISO 19115-2	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 2 : EXTENSIONS POUR L'ACQUISITION ET LE TRAITEMENT
ISO 19130.2	INFORMATION GÉOGRAPHIQUE – MODÈLES DE CAPTEURS D'IMAGES DE GÉOPOSITIONNEMENT – PARTIE 2 : SAR, INSAR, LIDAR ET SONAR
ISO 19130-1	INFORMATION GÉOGRAPHIQUE – MODÈLES DE CAPTEURS D'IMAGES ET GÉOPOSITIONNEMENT – PARTIE 1 : PRINCIPES DE BASE
ISO 19139.2	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – MISE EN OEUVRE PAR DES SCHÉMAS XML – PARTIE 2 : EXTENSION POUR L'IMAGERIE ET LES DONNÉES MAILLÉES
ISO 19150-4	INFORMATION GÉOGRAPHIQUE – ONTOLOGIE – PARTIE 4 : ONTOLOGIE DE SERVICE
ISO 19159.1	INFORMATION GÉOGRAPHIQUE – CALIBRATION ET VALIDATION DE CAPTEURS DE TÉLÉDÉTECTION – PARTIE 1 : CAPTEURS OPTIQUES
ISO 19159.3	INFORMATION GÉOGRAPHIQUE – CALIBRATION ET VALIDATION DE CAPTEURS DE TÉLÉDÉTECTION – PARTIE 3 : SAR/INSAR
ISO 19160.1	ADRESSAGE – PARTIE 1 : MODÈLE CONCEPTUEL
ISO 19160-1	ADRESSAGE – PARTIE 1 : MODÈLE CONCEPTUEL
ISO 19162	INFORMATION GÉOGRAPHIQUE – REPRÉSENTATION TEXTUELLE BIEN LISIBLE DE SYSTÈMES DE RÉFÉRENCE PAR COORDONNÉES
ISO 19165.1	INFORMATION GÉOGRAPHIQUE – ARCHIVAGE DES DONNÉES NUMÉRIQUES ET DES MÉTADONNÉES – PARTIE 1 : PRINCIPES FONDAMENTAUX
ISO 19165-1	INFORMATION GÉOGRAPHIQUE – ARCHIVAGE DES DONNÉES NUMÉRIQUES ET DES MÉTADONNÉES – PARTIE 1 : PRINCIPES FONDAMENTAUX

ISO 19289	QUALITÉ DE L'AIR – MÉTÉOROLOGIE – CLASSIFICATIONS DES SITES POUR LES STATIONS TERRESTRES D'OBSERVATION
ISO 19445	TECHNOLOGIE GRAPHIQUE – MÉTADONNÉES POUR LE FLUX DE TRAVAIL DES ARTS GRAPHIQUES – MÉTADONNÉES XMP POUR LA RELECTURE DE DOCUMENT ET D'IMAGE
ISO 19593-1	TECHNOLOGIE GRAPHIQUE – UTILISATION DU PDF POUR ASSOCIER LES ÉTAPES DE TRAITEMENT ET LES DONNÉES DE CONTENU – PARTIE 1 : ÉTAPES DE TRAITEMENT 2016
ISO 20614	INFORMATION ET DOCUMENTATION – PROTOCOLE D'ÉCHANGE DE DONNÉES POUR L'INTEROPÉRABILITÉ ET LA PRÉSERVATION
ISO 20616-2	TECHNOLOGIE GRAPHIQUE – FORMAT DE FICHIER POUR LE CONTRÔLE QUALITÉ ET LES MÉTADONNÉES – PARTIE 2 : PQX (PRINT QUALITY EXCHANGE)
ISO 2108	INFORMATION ET DOCUMENTATION – NUMÉRO INTERNATIONAL NORMALISÉ DU LIVRE (ISBN)
ISO 21812-1	TECHNOLOGIE GRAPHIQUE – MÉTADONNÉES DES PRODUITS D'IMPRESSION POUR LES FICHIERS PDF – PARTIE 1 : ARCHITECTURE ET EXIGENCES PRINCIPALES POUR LES MÉTADONNÉES
ISO 23081-1	INFORMATION ET DOCUMENTATION – PROCESSUS DE GESTION DES DOCUMENTS D'ACTIVITÉ – MÉTADONNÉES POUR LES DOCUMENTS D'ACTIVITÉ – PARTIE 1 : PRINCIPES
ISO 24097-1	UTILISATION DES SERVICES DU WEB (LIVRAISON DE MACHINE À MACHINE) POUR LA LIVRAISON DE SERVICES ITS – PARTIE 1 : RÉALISATION DES SERVICES DU WEB INTEROPÉRABLES
ISO 24619	GESTION DES RESSOURCES LINGUISTIQUES – IDENTIFICATION ET ACCÈS PÉRENNES
ISO 24622-2	GESTION DES RESSOURCES LINGUISTIQUES – COMPOSANTE INFRASTRUCTURE DE MÉTADONNÉES (CMDI) – PARTIE 2 : COMPOSANTE LINGUISTIQUE SPÉCIFIQUE AUX MÉTADONNÉES
ISO 25577	INFORMATION ET DOCUMENTATION – MARCXCHANGE
ISO 26324	INFORMATION ET DOCUMENTATION – SYSTÈME D'IDENTIFIANT NUMÉRIQUE D'OBJET
ISO 27730	INFORMATION ET DOCUMENTATION – IDENTIFIANT INTERNATIONAL NORMALISÉ DES COLLECTIONS (ISCI)
ISO 28258	QUALITÉ DU SOL – ÉCHANGE NUMÉRIQUE DE DONNÉES RELATIVES AU SOL
ISO 28500	INFORMATION ET DOCUMENTATION – FORMAT DE FICHIER WARC
ISO 639-4	CODES POUR LA REPRÉSENTATION DES NOMS DE LANGUE – PARTIE 4 : PRINCIPES GÉNÉRAUX POUR LE CODAGE DE LA REPRÉSENTATION DES NOMS DE LANGUE ET D'ENTITÉS CONNEXES, ET LIGNES DIRECTRICES POUR LA MISE EN OEUVRE
ISO 8	[Disponible uniquement en anglais]
ISO TR 13054	GESTION DES CONNAISSANCES DES NORMES EN INFORMATION DE LA SANTÉ
ISO TR 13128	Informatique de santé – Fédération d'enregistrement de documents cliniques
ISO TR 17321-2	TECHNOLOGIE GRAPHIQUE ET PHOTOGRAPHIE – CARACTÉRISATION DE LA COULEUR DES APPAREILS PHOTONUMÉRIQUES – PARTIE 2 : CONSIDÉRATIONS POUR DÉTERMINER LES TRANSFORMATIONS D'ANALYSE DE SCÈNE
ISO TR 23081-3	INFORMATION ET DOCUMENTATION – GESTION DES MÉTADONNÉES POUR L'INFORMATION ET LES DOCUMENTS – PARTIE 3 : MÉTHODE D'AUTO-ÉVALUATION
ISO TR 24097-2	[Disponible uniquement en anglais]
ISO TR 24097-3	[Disponible uniquement en anglais]
ISO TS 13972	INFORMATIQUE DE SANTÉ – MODÈLES CLINIQUES DÉTAILLÉS, CARACTÉRISTIQUES ET PROCESSUS
ISO TS 15926-12	SYSTÈMES D'AUTOMATISATION INDUSTRIELLE ET INTÉGRATION – INTÉGRATION DE DONNÉES DE CYCLE DE VIE POUR LES INDUSTRIES DE "PROCESS", Y COMPRIS LES USINES DE PRODUCTION DE PÉTROLE ET DE GAZ – PARTIE 12 : ONTOLOGIE D'INTÉGRATION DE CYCLE DE VIE REPRÉSENTÉE DANS LE LANGAGE D'ONTOLOGIE DU WEB (OWL)
ISO TS 17439	INFORMATIQUE DE SANTÉ – DÉVELOPPEMENT DES TERMES ET DÉFINITIONS POUR LES GLOSSAIRES D'INFORMATIQUE DE SANTÉ
ISO TS 17948	INFORMATIQUE DE SANTÉ – MÉTADONNÉES DE LITTÉRATURE DE LA MÉDECINE TRADITIONNELLE CHINOISE

ISO TS 19115-3	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 3 : MISE EN OEUVRE PAR DES SCHÉMAS XML
ISO TS 19159-2	INFORMATION GÉOGRAPHIQUE – CALIBRATION ET VALIDATION DE CAPTEURS DE TÉLÉDÉTECTION – PARTIE 2 : LIDAR
ISO TS 19159-3	INFORMATION GÉOGRAPHIQUE – CALIBRATION ET VALIDATION DE CAPTEURS DE TÉLÉDÉTECTION – PARTIE 3 : SAR/INSAR
ISO TS 20428	INFORMATIQUE DE SANTÉ – ÉLÉMENTS DE DONNÉES ET LEURS MÉTADONNÉES POUR DÉCRIRE L'INFORMATION STRUCTURÉE DE LA SÉQUENCE GÉNOMIQUE CLINIQUE DANS LES DOSSIERS DE SANTÉ ÉLECTRONIQUES
ISO TS 21526	INFORMATIQUE DE SANTÉ – EXIGENCES RELATIVES AUX RÉFÉRENTIELS DE MÉTADONNÉES (METAREP)
ISO/IEC 11179-1	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 1 : CADRE DE RÉFÉRENCE
ISO/IEC 11179-5	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 5 : PRINCIPES DE DÉNOMINATION
ISO/IEC 11179-6	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 6 : ENREGISTREMENT DES DONNÉES
ISO/IEC 14957	TECHNOLOGIES DE L'INFORMATION – REPRÉSENTATION DES VALEURS DES ÉLÉMENTS DE DONNÉES – NOTATION DU FORMAT
ISO/IEC 15444-2	[Disponible uniquement en anglais]
ISO/IEC 15444-5	[Disponible uniquement en anglais]
ISO/IEC 15444-6	TECHNOLOGIES DE L'INFORMATION – SYSTÈME DE CODAGE D'IMAGES JPEG 2000 – PARTIE 6 : FORMAT DE FICHIER D'IMAGE DE COMPOSANT
ISO/IEC 15444-8	[Disponible uniquement en anglais]
ISO/IEC 16500-6	TECHNOLOGIES DE L'INFORMATION – SYSTÈMES AUDIOVISUELS NUMÉRIQUES GÉNÉRIQUES – PARTIE 6 : REPRÉSENTATION DES INFORMATIONS
ISO/IEC 19566-5	TECHNOLOGIES DE L'INFORMATION – SYSTÈMES JPEG – PARTIE 5 : FORMAT UNIVERSEL DE FICHIER DE MÉTADONNÉES POUR JPEG (JUMBF)
ISO/IEC 19763-5	TECHNOLOGIES DE L'INFORMATION – CADRE DU MÉTAMODÈLE POUR L'INTEROPÉRABILITÉ (MFI) – PARTIE 5 : MÉTAMODÈLE POUR L'ENREGISTREMENT DU MODÈLE DE PROCÉDÉ
ISO/IEC 19763-6	TECHNOLOGIES DE L'INFORMATION – CADRE DU MÉTAMODÈLE POUR L'INTEROPÉRABILITÉ (MFI) – PARTIE 6 : RÉSUMÉ REGISTRY
ISO/IEC 19788-7	TECHNOLOGIES DE L'INFORMATION – APPRENTISSAGE, ÉDUCATION ET FORMATION – MÉTADONNÉES POUR RESSOURCES D'APPRENTISSAGE – PARTIE 5 : ÉLÉMENTS PÉDAGOGIQUES
ISO/IEC 19788-8	TECHNOLOGIE DE L'INFORMATION – APPRENTISSAGE, ÉDUCATION ET FORMATION – MÉTADONNÉES POUR RESSOURCES D'APPRENTISSAGE – PARTIE 8 : ÉLÉMENTS DE DONNÉES POUR LES ENREGISTREMENTS MLR
ISO/IEC 19788-9	TECHNOLOGIE DE L'INFORMATION – APPRENTISSAGE, ÉDUCATION ET FORMATION – MÉTADONNÉES POUR RESSOURCES D'APPRENTISSAGE – PARTIE 9 : ÉLÉMENTS DE DONNÉES POUR LES PERSONNES
ISO/IEC 19794-13	TECHNOLOGIES DE L'INFORMATION – FORMATS D'ÉCHANGES DE DONNÉES BIOMÉTRIQUES – PARTIE 13 : DONNÉES RELATIVES À LA VOIX
ISO/IEC 20248	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES D'IDENTIFICATION AUTOMATIQUE ET DE CAPTURE DE DONNÉES – STRUCTURES DE DONNÉES – MÉTA-STRUCTURE DE SIGNATURE NUMÉRIQUE
ISO/IEC 20944-2	TECHNOLOGIES DE L'INFORMATION – INTEROPÉRABILITÉ ET LIAISONS DES REGISTRES DE MÉTADONNÉES (MDR-IB) – PARTIE 2 : LIAISONS DE CODAGE
ISO/IEC 20944-3	TECHNOLOGIES DE L'INFORMATION – INTEROPÉRABILITÉ ET LIAISONS DES REGISTRES DE MÉTADONNÉES (MDR-IB) – PARTIE 3 : LIAISONS API
ISO/IEC 20944-4	TECHNOLOGIES DE L'INFORMATION – INTEROPÉRABILITÉ ET LIAISONS DES REGISTRES DE MÉTADONNÉES (MDR-IB) – PARTIE 4 : LIAISONS DE PROTOCOLES

ISO/IEC 20944-5	TECHNOLOGIES DE L'INFORMATION – INTEROPÉRABILITÉ ET LIAISONS DES REGISTRES DE MÉTADONNÉES (MDR-IB) – PARTIE 5 : PROFILS
ISO/IEC 21000-22	TECHNOLOGIES DE L'INFORMATION – CADRE MULTIMÉDIA (MPEG-21) – PARTIE 22 : DESCRIPTION DE L'UTILISATEUR
ISO/IEC 22602	[Disponible uniquement en anglais]
ISO/IEC 23000-22	TECHNOLOGIES DE L'INFORMATION – FORMAT POUR APPLICATION MULTIMÉDIA (MPEG-A) – PARTIE 22 : FORMAT POUR APPLICATION À IMAGES MULTIPLES (MIAF) – AMENDEMENT 1 : LOGICIEL DE RÉFÉRENCE ET CONFORMITÉ POUR LE FORMAT POUR APPLICATION À IMAGES MULTIPLES
ISO/IEC 23001-10	TECHNOLOGIES DE L'INFORMATION – TECHNOLOGIES DES SYSTÈMES MPEG – PARTIE 10 : TRANSPORT DE MÉTRIQUES DE MÉTADONNÉES DE TEMPORISATION DE SUPPORTS AU FORMAT DE FICHIER DE SUPPORT EN BASE ISO
ISO/IEC 23001-11	TECHNOLOGIES DE L'INFORMATION – TECHNOLOGIES DES SYSTÈMES MPEG – PARTIE 11 : CONSOMMATION DES SUPPORTS ÉCONERGÉTIQUES (MÉTADONNÉES VERTES)
ISO/IEC 23001-13	[Disponible uniquement en anglais]
ISO/IEC 23001-7	TECHNOLOGIES DE L'INFORMATION – TECHNOLOGIES DES SYSTÈMES MPEG – PARTIE 7 : CRYPTAGE COMMUN DES FICHIERS AU FORMAT DE FICHIER DE MÉDIAS DE LA BASE ISO
ISO/IEC 23005-4	TECHNOLOGIES DE L'INFORMATION – CONTRÔLE ET CONTEXTE DE SUPPORTS – PARTIE 4 : CARACTÉRISTIQUES D'OBJET DU MONDE VIRTUEL
ISO/IEC 23008-12	TECHNOLOGIES DE L'INFORMATION – CODAGE À HAUTE EFFICACITÉ ET LIVRAISON DES MEDIAS DANS DES ENVIRONNEMENTS HÉTÉROGÈNES – PARTIE 12 : FORMAT DE FICHIER D'IMAGE – RECTIFICATIF TECHNIQUE 1
ISO/IEC 23008-3	TECHNOLOGIES DE L'INFORMATION – CODAGE À HAUTE EFFICACITÉ ET LIVRAISON DES MEDIAS DANS DES ENVIRONNEMENTS HÉTÉROGÈNES – PARTIE 3 : AUDIO 3D – AMENDEMENT 2 : PROFIL DE BASE AUDIO 3D, CORRECTIONS ET AMÉLIORATIONS
ISO/IEC 23092-3	TECHNOLOGIE DE L'INFORMATION – REPRÉSENTATION DES INFORMATIONS GÉNOMIQUES – PARTIE 3 : MÉTADONNÉES ET INTERFACES DE PROGRAMMATION D'APPLICATION (API)
ISO/IEC 24800-5	TECHNOLOGIES DE L'INFORMATION – JPSEARCH – PARTIE 5 : FORMAT D'ÉCHANGE DE DONNÉES ENTRE RÉFÉRENTIELS D'IMAGES
ISO/IEC 29500-2	TECHNOLOGIES DE L'INFORMATION – DESCRIPTION DES DOCUMENTS ET LANGAGES DE TRAITEMENT – FORMATS DE FICHIER "OFFICE OPEN XML" – PARTIE 2 : CONVENTIONS DE PAQUETAGE OUVERT
ISO/IEC 40260	TECHNOLOGIES DE L'INFORMATION – ADRESSAGE DE SERVICES WEB 1.0 – MÉTADONNÉES
ISO/IEC TR 11179-2	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 2 : CLASSIFICATION
ISO/IEC TR 15938-11	TECHNOLOGIES DE L'INFORMATION – INTERFACE DE DESCRIPTION DU CONTENU MULTIMÉDIA – PARTIE 11 : SCHÉMAS DU PROFIL MPEG-7
ISO/IEC TR 15938-8	TECHNOLOGIES DE L'INFORMATION – INTERFACE DE DESCRIPTION DU CONTENU MULTIMÉDIA – PARTIE 8 : EXTRACTION ET UTILISATION DES DESCRIPTIONS MPEG-7 – AMENDEMENT 6 : EXTRACTION ET CORRESPONDANCE DES OUTILS DE SIGNATURE VIDÉO
ISO/IEC TR 19583-1	TECHNOLOGIES DE L'INFORMATION – CONCEPTS ET UTILISATION DES MÉTADONNÉES – PARTIE 1 : CONCEPTS LIÉS AUX MÉTADONNÉES
ISO/IEC TR 19583-22	TECHNOLOGIES DE L'INFORMATION – CONCEPTS ET UTILISATION DES MÉTADONNÉES – PARTIE 22 : L'ENREGISTRANT ET MAPPANT DE PROCESSUS DE DÉVELOPPEMENT À L'AIDE DE ISO/IEC 19763
ISO/IEC TR 20943-1	TECHNOLOGIES DE L'INFORMATION – PROCÉDURES EN VUE D'OBTENIR LA COHÉRENCE DU CONTENU D'UN REGISTRE DE METADONNÉES – PARTIE 1 : ÉLÉMENTS DE DONNÉES
ISO/IEC TR 20943-3	TECHNOLOGIES DE L'INFORMATION – PROCÉDURES POUR RÉALISER LA CONSISTANCE DU CONTENU DE L'ENREGISTREMENT DES MÉTADONNÉES – PARTIE 3 : DOMAINES DE VALEUR
ISO/IEC TR 20943-5	TECHNOLOGIES DE L'INFORMATION —PROCÉDURES POUR RÉALISER LA CONSISTANCE DU CONTENU DE L'ENREGISTREMENT DES MÉTADONNÉES – PARTIE 5 : PROCÉDURE DE MAPPAGE DES MÉTADONNÉES
ISO/IEC TR 20943-6	TECHNOLOGIES DE L'INFORMATION —PROCÉDURES POUR RÉALISER LA CONSISTANCE DU CONTENU DE L'ENREGISTREMENT DES MÉTADONNÉES – PARTIE 6 : CADRE POUR GÉNÉRER DES ONTOLOGIES

ISO/IEC TR 21000-11	TECHNOLOGIES DE L'INFORMATION – CADRE MULTIMÉDIA (MPEG-21) – PARTIE 11 : OUTILS D'ÉVALUATION RELATIFS AUX TECHNOLOGIES D'ASSOCIATION PERSISTANTE
ISO/IEC TS 11179-30	[Disponible uniquement en anglais]
ISO/IEC/IEEE 23026	Ingénierie des systèmes et du logiciel – Ingénierie et gestion de sites web pour les systèmes, logiciels et services d'information
ISO/TR 23081-3	INFORMATION ET DOCUMENTATION – GESTION DES MÉTADONNÉES POUR L'INFORMATION ET LES DOCUMENTS – PARTIE 3 : MÉTHODE D'AUTO-ÉVALUATION
ISO/TS 19115-3	Information géographique – Métadonnées – Partie 3 : Mise en oeuvre par des schémas XML
ISO/TS 19130	Information géographique – Modèles de capteurs d'images de géopositionnement
ISO/TS 19130-2	Information géographique – Modèles de capteurs d'images de géopositionnement – Partie 2 : SAR, InSAR, lidar et sonar
ISO/TS 19139	Information géographique – Métadonnées – Implémentation de schémas XML
ISO/TS 19139-2	Information géographique – Métadonnées – Mise en oeuvre par des schémas XML – Partie 2 : Extension pour l'imagerie et les données maillées
ITU-R BS.2076-2	Modèle de définition audio
ITU-R BS.2088-1	Format des fichiers longue durée pour l'échange international de programmes audio avec métadonnées
ITU-T F.750	Cadre général applicable aux métadonnées
ITU-T T.804	Technologies de l'information – Système de codage d'image JPEG 2000 : logiciels de référence
ITU-T T.805	Technologies de l'information – Système de codage d'images JPEG 2000 : Format de fichier d'image composite
ITU-T T.808	Technologies de l'information – Système de codage d'images JPEG 2000 : outils d'interactivité, interfaces de programmes d'application et protocoles
ITU-T X.1276	Protocole d'amélioration de l'authentification et métadonnées – Version 1.0
ITU-T Y.3603	Mégadonnées – Exigences et modèle conceptuel applicables aux métadonnées pour les catalogues de données
ULC CAN/ULC-S316-14	NORME SUR LA PERFORMANCE DES SYSTÈMES DE SURVEILLANCE VIDÉO
ISO/IEC TR 29163-1	TECHNOLOGIES DE L'INFORMATION – MODÈLE DE RÉFÉRENCE D'OBJET DE CONTENU PARTAGEABLE (SCORM®) 2004 3E ÉDITION – PARTIE 1 : EXPOSÉ GÉNÉRAL VERSION 1.1
ITU-T X.1255	Cadre pour la découverte des informations relatives à la gestion d'identité
ISO/IEC TR 20547-2	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 2 : CAS PRATIQUES ET EXIGENCES DÉRIVÉES
IEEE 2413	[Disponible uniquement en anglais]
ISO/IEC TR 29163-2	TECHNOLOGIES DE L'INFORMATION – MODÈLE DE RÉFÉRENCE D'OBJET DE CONTENU PARTAGEABLE (SCORM®) 2004 3E ÉDITION – PARTIE 2 : MODÈLE D'AGRÉGATION DE CONTENU VERSION 1.1
ISO/IEC 19286	CARTES D'IDENTIFICATION – CARTES À CIRCUIT INTÉGRÉ – PROTOCOLES ET SERVICES RENFORÇANT LA PROTECTION DES DONNÉES PERSONNELLES
ISO/IEC 30141	Architecture de référence de l'Internet des objets (IoT RA)
ISO/IEC 30118-2	TECHNOLOGIES DE L'INFORMATION – SPÉCIFICATION DE LA FONDATION POUR LA CONNECTIVITÉ OUVERTE (FONDATION OCF) – PARTIE 2 : SPÉCIFICATION DE SÉCURITÉ
ISO/IEC 23271	TECHNOLOGIES DE L'INFORMATION – INFRASTRUCTURE COMMUNE DE LANGAGE (ICL)
ISO/IEC 30118-1	TECHNOLOGIES DE L'INFORMATION – SPÉCIFICATION DE LA FONDATION POUR LA CONNECTIVITÉ OUVERTE (FONDATION OCF) – PARTIE 1 : SPÉCIFICATION DU COEUR
ISO 16175.2	INFORMATION ET DOCUMENTATION – PRINCIPES ET EXIGENCES FONCTIONNELLES POUR LES ENREGISTREMENTS DANS LES ENVIRONNEMENTS ÉLECTRONIQUES DE BUREAU – PARTIE 3 : LIGNES DIRECTRICES ET EXIGENCES FONCTIONNELLES POUR LES ENREGISTREMENTS DANS LES SYSTÈMES D'ENTREPRISE

ISO 16175-2	INFORMATION ET DOCUMENTATION – PRINCIPES ET EXIGENCES FONCTIONNELLES POUR LES ENREGISTREMENTS DANS LES ENVIRONNEMENTS ÉLECTRONIQUES DE BUREAU – PARTIE 2 : LIGNES DIRECTRICES ET EXIGENCES FONCTIONNELLES POUR LES SYSTÈMES DE MANAGEMENT DES ENREGISTREMENTS NUMÉRIQUES
ISO/IEC 23270	TECHNOLOGIES DE L'INFORMATION – LANGAGES DE PROGRAMMATION – C#
ISO/IEC 19763-1	TECHNOLOGIES DE L'INFORMATION – CADRE DU MÉTAMODÈLE POUR L'INTEROPÉRABILITÉ (MFI) – PARTIE 1 : STRUCTURE
ANSI INCITS 530	[Disponible uniquement en anglais]
ISO/IEC 18384-1	TECHNOLOGIE DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE POUR L'ARCHITECTURE ORIENTÉE SERVICE (SOA RA) – PARTIE 1 : TERMINOLOGIE ET CONCEPTS POUR SOA
ISO/IEC TR 30102	TECHNOLOGIE DE L'INFORMATION – L'PLATE-FORMES ET SERVICES D'APPLICATIONS DISTRIBUÉES (DAPS) – PRINCIPES TECHNIQUES GÉNÉRAUX DE L'ARCHITECTURE ORIENTÉE SERVICES
ISO/IEC TR 22417	[Disponible uniquement en anglais]
BSI PAS 185	[Disponible uniquement en anglais]
ISO/IEC 23271	TECHNOLOGIES DE L'INFORMATION – INFRASTRUCTURE COMMUNE DE LANGAGE (ICL)
IEC 62656-1	Enregistrement d'ontologie de produits normalisés et transfert par tableurs – Partie 1 : Structure logique pour les paquets de données
IEC 82045-1	Gestion de documents – Partie 1 : Principes et méthodes
ISO 19115	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ISO/IEC 11179-3	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 3 : MÉTAMODÈLE DE REGISTRE ET ATTRIBUTS DE BASE – AMENDEMENT 1
ISO/IEC 20802-1	TECHNOLOGIES DE L'INFORMATION – PROTOCOLE DE DONNÉES OUVERTES (ODATA) V4.0 – PARTIE 1 : BASE
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CIOSC/PAS 100-4:2020	Gouvernance De Données – Partie 4 : Spécification pour une infrastructure adaptable d'accès à distance
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 106-1	Découverte des jumeaux numériques pour les environnements bâtis
IEEE 1667-2018	[Disponible uniquement en anglais]
IEEE P2957	[Disponible uniquement en anglais]
IEEE P1951.1	[Disponible uniquement en anglais]
IEEE P1752	[Disponible uniquement en anglais]
n/a	Statistique Canada Normes statistiques (Concepts, classifications et variables)
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]

Question clé 14
couplage de données

API BULL 1178	[Disponible uniquement en anglais]
ETSI TR 103 290	[Disponible uniquement en anglais]
ETSI TR 103 376	[Disponible uniquement en anglais]
ETSI TR 103 536	[Disponible uniquement en anglais]
ETSI TS 118 101	[Disponible uniquement en anglais]
ISO 22857	Informatique de santé – Lignes directrices sur la protection des données pour faciliter les flux d'information sur la santé du personnel de part et d'autre des frontières
ISO 27799	INFORMATIQUE DE SANTÉ – MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION RELATIVE À LA SANTÉ EN UTILISANT L'ISO/IEC 27002
ISO TR 18638	INFORMATIQUE DE SANTÉ – COMPOSANTES ÉDUCATIVES DESTINÉES À GARANTIR LA CONFIDENTIALITÉ DES INFORMATIONS RELATIVES À LA SANTÉ
ISO/IEC 19941	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – INTEROPÉRABILITÉ ET PORTABILITÉ
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO/IEC 20006.1	TECHNOLOGIES DE L'INFORMATION POUR L'APPRENTISSAGE, L'ÉDUCATION ET LA FORMATION – MODÈLE D'INFORMATION POUR LES COMPÉTENCES – PARTIE 1 : CADRE GÉNÉRAL DES COMPÉTENCES ET MODÈLE D'INFORMATION
ISO/IEC 20006-1	TECHNOLOGIES DE L'INFORMATION POUR L'APPRENTISSAGE, L'ÉDUCATION ET LA FORMATION – MODÈLE D'INFORMATION POUR LES COMPÉTENCES – PARTIE 1 : CADRE GÉNÉRAL DES COMPÉTENCES ET MODÈLE D'INFORMATION
ISO/IEC 21823-1	INTERNET DES OBJETS (IOT) – INTEROPÉRABILITÉ DES SYSTÈMES IOT – PARTIE 1 : CADRE MÉTHODOLOGIQUE
ISO/IEC 38505.2	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – PARTIE 2 : IMPLICATIONS DE L'ISO/IEC 38505-1 POUR LA GESTION DES DONNÉES
ISO/IEC TR 20547-2	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 2 : CAS PRATIQUES ET EXIGENCES DÉRIVÉES
ISO/IEC TR 20547-5	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 5 : FEUILLE DE ROUTE POUR LES NORMES
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC TS 19763-13	TECHNOLOGIES DE L'INFORMATION – CADRE DU MÉTAMODÈLE POUR L'INTEROPÉRABILITÉ (MFI) – PARTIE 13 : MÉTAMODÈLE POUR L'ENREGISTREMENT DE LA CONCEPTION DES FORMULAIRES
ISO/IEC/IEEE 24748-7	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – GESTION DU CYCLE DE VIE – PARTIE 7 : APPLICATION DE L'INGÉNIERIE DES SYSTÈMES AUX PROGRAMMES DE DÉFENSE
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO/TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ITU-T SERIES Y SUPP 40	[Disponible uniquement en anglais]
ITU-T X.1040	Architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique
ITU-T X.1363	[Disponible uniquement en anglais]
ITU-T X.814	Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts : cadre de confidentialité
ITU-T Y.4203	Exigences relatives à la description des objets dans l'Internet des objets

ITU-T Z.100 ANNEXE F1	Langage de description et de spécification – Présentation générale de SDL-2010 – Définition formelle du langage SDL : Présentation générale
ITU-T Z.100 ANNEXE F3	Langage de description et de spécification – Présentation générale de SDL-2010 – Définition formelle du langage SDL-2010 : Sémantique dynamique

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

IEEE Std 1888.4-2016	NORME SUR LA PERFORMANCE DES SYSTÈMES DE SURVEILLANCE VIDÉO
IEEE P2030	NORME SUR LA PERFORMANCE DES SYSTÈMES DE SURVEILLANCE VIDÉO
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-5	NORME SUR LA PERFORMANCE DES SYSTÈMES DE SURVEILLANCE VIDÉO

Question clé 15
marquage manuel des données

BSI BS 5701-2	[Disponible uniquement en anglais]
ISO 19731	Analytique numérique et analyses web pour les besoins d'études de marché, études sociales et d'opinion – Vocabulaire et exigences de service
ISO/IEC 19790	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – EXIGENCES DE SÉCURITÉ POUR LES MODULES CRYPTOGRAPHIQUES
ISO/IEC TR 27550	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – INGÉNIERIE DE LA VIE PRIVÉE POUR LES PROCESSUS DU CYCLE DE VIE DES SYSTÈMES
ISO/IEC TS 20540	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – TEST DE MODULES CRYPTOGRAPHIQUES DANS LEUR ENVIRONNEMENT D'EXPLOITATION

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	NORME SUR LA PERFORMANCE DES SYSTÈMES DE SURVEILLANCE VIDÉO
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada

Question clé 16
gestion des métadonnées

ASTM E2468	[Disponible uniquement en anglais]
BIS IS 15992	GESTION DES RESSOURCES LANGAGIÈRES – COMPOSANTE INFRASTRUCTURE DE MÉTADONNÉES (CMDI) – PARTIE 1 : COMPOSANT MODÈLE DE MÉTADONNÉES
ETSI GR NFV-SEC 003	[Disponible uniquement en anglais]
IEC 82045-1	Établissement des documents utilisés en électrotechnique – Partie 1 : Règles
IEC 82045-2	Cadre pour les communications pour le marché de l'énergie – Partie 503 : Lignes directrices concernant les échanges de données du marché pour le profil défini dans l'IEC 62325-351
IEEE 1484.12.3	NAVIRES ET TECHNOLOGIE MARITIME – ÉNERGIE ÉOLIENNE OFFSHORE – FLUX D'INFORMATIONS DANS LA CHAÎNE D'APPROVISIONNEMENT
IEEE COMP	Exigences pour la gestion des données dans le réseau de gestion des télécommunications
IEEE STDVA24228	[Disponible uniquement en anglais]
ISO 15836	[Disponible uniquement en anglais]

ISO 15836-1	[Disponible uniquement en anglais]
ISO 15836-2	[Disponible uniquement en anglais]
ISO 17369	TECHNOLOGIES DE L'INFORMATION – INTERFACE DE DESCRIPTION DU CONTENU MULTIMÉDIA – PARTIE 2 : LANGAGE DE DÉFINITION DE DESCRIPTION (DDL)
ISO 24622-1	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – LIGNES DIRECTRICES POUR L'ÉVALUATION ET LE CHOIX DES OUTILS D'INGÉNIERIE LOGICIELLE
ISO 24622-2	Présentation générale des terminaux et systèmes d'extrémité de TVIP
ISO/IEC 11179-1	TECHNOLOGIES DE L'INFORMATION – APPRENTISSAGE, ÉDUCATION ET FORMATION – PAQUETAGE DU CONTENU – PARTIE 2 : LIAISON XML
ISO/IEC 11179-2	TECHNOLOGIES DE L'INFORMATION – CODAGE GÉNÉRIQUE DES IMAGES ANIMÉES ET DU SON ASSOCIÉ – PARTIE 1 : SYSTÈMES – RECTIFICATIF TECHNIQUE 1
ISO/IEC 11179-6	TECHNOLOGIES DE L'INFORMATION – PROTOCOLE DE DONNÉES OUVERTES (ODATA) V4.0 – PARTIE 2 : FORMAT ODATA JSON
ISO/IEC 23001-13	[Disponible uniquement en anglais]
ISO/IEC TR 20943-6	[Disponible uniquement en anglais]
SNZ SA/SNZ HB 168	Intergiciels de terminaux de TVIP centrés sur la radiodiffusion
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
IEEE P2957	[Disponible uniquement en anglais]
IEEE P2881	[Disponible uniquement en anglais]
IEEE P4002	[Disponible uniquement en anglais]
IEEE P4003	[Disponible uniquement en anglais]
IEEE IC17-006	[Disponible uniquement en anglais]
n/a	Statistique Canada Normes statistiques (Concepts, classifications et variables)
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]

Question clé 17
stratégies de politique de données organisationnelles et gestion des risques

ANSI X9.100-181	[Disponible uniquement en anglais]
ANSI X9.111	[Disponible uniquement en anglais]
API BULL 1178	[Disponible uniquement en anglais]
API PUBL 353	[Disponible uniquement en anglais]
API PUBL 4620	[Disponible uniquement en anglais]
ASCE GSP 98	[Disponible uniquement en anglais]
ASHRAE HVAC APPLICATIONS SI HANDBOOK	[Disponible uniquement en anglais]
ASTM E1714	[Disponible uniquement en anglais]
ASTM E2147	[Disponible uniquement en anglais]
ASTM E2842	[Disponible uniquement en anglais]

ASTM F3286	[Disponible uniquement en anglais]
ASTM F3449	[Disponible uniquement en anglais]
ASTM MNL19	[Disponible uniquement en anglais]
ASTM MNL58	[Disponible uniquement en anglais]
AWWA G410	[Disponible uniquement en anglais]
BSI BS 10008-2	[Disponible uniquement en anglais]
BSI BS 70000	[Disponible uniquement en anglais]
BSI PAS 197	[Disponible uniquement en anglais]
BSI PD 7505	[Disponible uniquement en anglais]
BSI PD 7506	[Disponible uniquement en anglais]
BSI PD 8100	[Disponible uniquement en anglais]
CEN 17255-2	Émissions de sources fixes – Systèmes d'acquisition et de traitement de données – Partie 2 : Spécification des exigences relatives aux systèmes d'acquisition et de traitement de données
CEN EN 50518	[Disponible uniquement en anglais]
CEN/TR 15584	Caractérisation des boues – Guide pour l'appréciation du risque, en relation notamment avec l'utilisation et l'élimination des boues
CEN/TR 16674	[Disponible uniquement en anglais]
CEN/TR 17370	[Disponible uniquement en anglais]
CEN/TS 17434	Air ambiant – Détermination de la distribution granulométrique de particules d'un aérosol atmosphérique à l'aide d'un spectromètre de granulométrie à mobilité électrique (MPSS)
CENELEC EN 50436-6	Éthylotests antidémarrage – Méthodes d'essai et exigences de performance – Partie 6 : Sécurité des données
CENELEC EN 50491-12-1	Exigences générales relatives aux systèmes électroniques pour les foyers domestiques et les bâtiments (HBES) et aux systèmes de gestion technique du bâtiment (SGTB) Réseau intelligent Spécification d'application Interface et cadre pour le client – Partie 12-1 : Interface entre le gestionnaire d'énergie pour le client (CEM, Customer Energy Manager) et le gestionnaire de ressources pour foyers domestiques/ bâtiments. Exigences et Architecture générales
CENELEC EN 50600-3-1	Technologie de l'information – Installation et infrastructures de centres de traitement de données – Partie 3-1 : Informations de gestion et de fonctionnement
CLSI QMS22	[Disponible uniquement en anglais]
DS DS/CWA 15847	[Disponible uniquement en anglais]
ETSI GS ISI 002	[Disponible uniquement en anglais]
ETSI TR 102 659-1	[Disponible uniquement en anglais]
ETSI TS 187 001	[Disponible uniquement en anglais]
GOST R 34.13	[Disponible uniquement en anglais]
IEC 60300-3-15	Gestion de la sûreté de fonctionnement – Partie 3-15 : Guide d'application – Ingénierie de la sûreté de fonctionnement des systèmes
IEC 62056-21	Equipements de mesure de l'énergie électrique – Echange des données pour la lecture des compteurs, le contrôle des tarifs et de la charge – Partie 21 : Echange des données directes en local
IEC 62443-2-1	Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 2-1 : Etablissement d'un programme de sécurité pour les systèmes d'automatisation et de commande industrielles
IEC 62962	Exigences spécifiques pour les délesteurs (LSE)
IEC/IEEE 82079-1	Élaboration des informations d'utilisation (instructions d'utilisation) des produits – Partie 1 : Principes et exigences générales
IEEE 1232.1	[Disponible uniquement en anglais]
IEEE 1455	[Disponible uniquement en anglais]

IEEE 1484.11.2	[Disponible uniquement en anglais]
IEEE 1685	[Disponible uniquement en anglais]
IEEE 1914.1	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
IEEE ICICLE	[Disponible uniquement en anglais]
ISO 14031	MANAGEMENT ENVIRONNEMENTAL – ÉVALUATION DE LA PERFORMANCE ENVIRONNEMENTALE – LIGNES DIRECTRICES
ISO 14644-2	SALLES PROPRES ET ENVIRONNEMENTS MAÎTRISÉS APPARENTÉS – PARTIE 1 : CLASSIFICATION DE LA PROPRETÉ PARTICULAIRE DE L'AIR
ISO 15638-21	SYSTÈMES INTELLIGENTS DE TRANSPORT – CADRE POUR APPLICATIONS TÉLÉMATIQUES COLLABORATIVES POUR VÉHICULES DE FRET COMMERCIAL RÉGLEMENTÉ (TARV) – PARTIE 21 : SURVEILLANCE DES VÉHICULES RÉGLEMENTÉS À L'AIDE DE CAPTEURS ROUTIERS ET DE DONNÉES COLLECTÉES DANS LES VÉHICULES POUR L'APPLICATION DES LOIS ET À D'AUTRES FINS
ISO 16598	STRUCTURES EN BOIS – CLASSIFICATION STRUCTURELLE POUR BOIS SCIÉS
ISO 16919	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – EXIGENCES POUR LES ORGANISMES D'AUDIT ET DE CERTIFICATION DES RÉFÉRENTIELS NUMÉRIQUES POTENTIELLEMENT DE CONFIANCE
ISO 17427-1	SYSTÈMES DE TRANSPORT INTELLIGENTS – SYSTÈMES DE TRANSPORT COOPÉRATIFS INTELLIGENTS – PARTIE 1 : RÔLES ET RESPONSABILITÉS DANS LE CONTEXTE DES STI FONDÉS SUR L'ARCHITECTURE
ISO 17892-12	RECONNAISSANCE ET ESSAIS GÉOTECHNIQUES – ESSAIS DE LABORATOIRE SUR LES SOLS – PARTIE 12 : DÉTERMINATION DES LIMITES DE LIQUIDITÉ ET DE PLASTICITÉ
ISO 22307	SERVICES FINANCIERS – ÉVALUATION DE L'IMPACT PRIVÉ
ISO 30302	INFORMATION ET DOCUMENTATION – SYSTÈME DE GESTION DES DOCUMENTS D'ACTIVITÉ – LIGNES DIRECTRICES DE MISE EN OEUVRE
ISO 41001	FACILITY MANAGEMENT – SYSTÈMES DE MANAGEMENT – EXIGENCES AVEC RECOMMANDATIONS D'UTILISATION
ISO 8000-2	QUALITÉ DES DONNÉES – PARTIE 2 : VOCABULAIRE
ISO 8000-61	Qualité des données – Partie 61 : Gestion de la qualité des données : Modèle de référence des procédés
ISO TR 23791	VÉHICULES ROUTIERS – WEB SERVICES DU VÉHICULE ÉTENDU (EXVE) – RÉSULTATS DE L'ÉVALUATION DES RISQUES DE LA SÉRIE DE NORMES ISO 20078
ISO TS 21547	INFORMATIQUE DE SANTÉ – EXIGENCES DE SÉCURITÉ POUR L'ARCHIVAGE DES DOSSIERS DE SANTÉ ÉLECTRONIQUES – PRINCIPES
ISO/HL7 27951 cd-rom	Informatique de santé – Services de terminologie commune, Version 1
ISO/IEC 13211-1	TECHNOLOGIES DE L'INFORMATION – LANGAGES DE PROGRAMMATION – PROLOG – PARTIE 1 : NOYAU GÉNÉRAL – RECTIFICATIF TECHNIQUE 3
ISO/IEC 15504-6	TECHNOLOGIES DE L'INFORMATION – ÉVALUATION DES PROCÉDÉS – PARTIE 6 : UN EXEMPLE DE MODÈLE D'ÉVALUATION DES PROCÉDÉS DU CYCLE DE VIE D'UN SYSTÈME
ISO/IEC 19778-1	TECHNOLOGIES DE L'INFORMATION – APPRENTISSAGE, ÉDUCATION ET FORMATION – TECHNOLOGIES COLLABORATIVES – LIEU DE TRAVAIL COLLABORATIF – PARTIE 1 : MODÈLE DE DONNÉES DU LIEU DE TRAVAIL COLLABORATIF
ISO/IEC 19941	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – INTEROPÉRABILITÉ ET PORTABILITÉ
ISO/IEC 20547-3	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES MÉGADONNÉES – PARTIE 3 : ARCHITECTURE DE RÉFÉRENCE
ISO/IEC 20748.4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4 :
ISO/IEC 21878	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR LA CONCEPTION ET L'IMPLÉMENTATION SÉCURISÉES DES SERVEURS VIRTUALISÉS

ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 27002	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CODE DE BONNE PRATIQUE POUR LE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION
ISO/IEC 27017	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CODE DE BONNES PRATIQUES POUR LES CONTRÔLES DE SÉCURITÉ DE L'INFORMATION FONDÉS SUR L'ISO/IEC 27002 POUR LES SERVICES DU NUAGE
ISO/IEC 27018	Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
ISO/IEC 27701	TECHNIQUES DE SÉCURITÉ – EXTENSION D'ISO/IEC 27001 ET ISO/IEC 27002 AU MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE – EXIGENCES ET LIGNES DIRECTRICES
ISO/IEC 29151	Technologies de l'information – Techniques de sécurité – code de bonne pratique pour la protection des données à caractère personnel
ISO/IEC 38506	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – APPLICATION DE L'ISO/IEC 38500 À LA GOUVERNANCE DES INVESTISSEMENTS REPOSANT SUR LES TECHNOLOGIES DE L'INFORMATION
ISO/IEC 9075-2	TECHNOLOGIES DE L'INFORMATION – LANGAGES DE BASE DE DONNÉES – SQL – PARTIE 2 : FONDATIONS (SQL/FONDATIONS) – RECTIFICATIF TECHNIQUE 1
ISO/IEC TR 24028	TECHNOLOGIES DE L'INFORMATION – INTELLIGENCE ARTIFICIELLE – EXAMEN D'ENSEMBLE DE LA FIABILITÉ EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE
ISO/IEC TR 24729-4	TECHNOLOGIES DE L'INFORMATION – IDENTIFICATION DE RADIOFRÉQUENCES POUR LA GESTION D'ITEMS – LIGNES DIRECTRICES POUR LA MISE EN OEUVRE – PARTIE 4 : SÉCURITÉ DES DONNÉES DE REPÈRE
ISO/IEC TS 18508	TECHNOLOGIES DE L'INFORMATION – CARACTÉRISTIQUES PARALLÈLES SUPPLÉMENTAIRES EN FORTRAN
ISO/IEC TS 33072	INFORMATION TECHNOLOGY – PROCESS ASSESSMENT – PROCESS CAPABILITY ASSESSMENT MODEL FOR INFORMATION SECURITY MANAGEMENT
ISO/TR 18638	INFORMATIQUE DE SANTÉ – COMPOSANTES ÉDUCATIVES DESTINÉES À GARANTIR LA CONFIDENTIALITÉ DES INFORMATIONS RELATIVES À LA SANTÉ
ISO/TS 17427	Systèmes intelligents de transport – Systèmes coopératifs – Rôles et responsabilités dans le contexte des ITS fondés sur l'architecture de systèmes coopératifs
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO/TS 21547	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Principes
ISO/TS 8000-65	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 49	[Disponible uniquement en anglais]
ITU-T X.1040	Architecture de référence de sécurité pour la gestion, tout au long de leur cycle de vie, des données sur les transactions de commerce électronique
ITU-T X.1086	Procédures de protection télébiométriques – Lignes directrices relatives aux mesures techniques et de gestion pour la sécurité des données biométriques
ITU-T X.1603	[Disponible uniquement en anglais]
ITU-T X.1641	[Disponible uniquement en anglais]
ITU-T Y.2330	Exigences relatives à l'évolution des réseaux de prochaine génération pour la prise en charge du service de données gratuites
ITU-T Y.3518	Informatique en nuage – Exigences fonctionnelles de la gestion de données inter-nuages
ITU-T Y.3518	Informatique en nuage – Exigences fonctionnelles de la gestion de données inter-nuages
ITU-T Y.3519	Informatique en nuage – Architecture fonctionnelle des mégadonnées en tant que service
ITU-T Y.3600	Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage

NEMA MITA CSP 1	[Disponible uniquement en anglais]
NEN NPR-CR 1832	[Disponible uniquement en anglais]
SAE GEIA-859A	[Disponible uniquement en anglais]
SAE GEIA-HB-649A	[Disponible uniquement en anglais]
SAE GEIA-HB-859	[Disponible uniquement en anglais]
SAE PT-182	[Disponible uniquement en anglais]
SNV SN CR 13694	[Disponible uniquement en anglais]
SNZ NZS 8153	[Disponible uniquement en anglais]
SNZ SA/SNZ HB 168	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
IEEE/ISO/IEC 29119-2-2013	[Disponible uniquement en anglais]
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données

Question clé 18
qualité des données et adaptation à l'utilisation

API BULL 1178	[Disponible uniquement en anglais]
CEN 16991	Cadre d'inspection basée sur les risques
IEC 31010	Management du risque – Techniques d'appréciation du risque
ISO 17369	DONNÉES STATISTIQUES ET ÉCHANGE DE MÉTADONNÉES (SDMX)
ISO 19115.1	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ISO 19115-1	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ISO 8000-100	QUALITÉ DES DONNÉES – PARTIE 100 : DONNÉES PERMANENTES : ÉCHANGE DES DONNÉES CARACTÉRISTIQUES : APERÇU GÉNÉRAL
ISO 8000-110	QUALITÉ DES DONNÉES – PARTIE 110 : DONNÉES PERMANENTES : ÉCHANGE DES DONNÉES CARACTÉRISTIQUES : SYNTAXE, SÉMANTIQUE, ENCODAGE ET CONFORMITÉ AUX SPÉCIFICATIONS DE DONNÉES
ISO 8000-115	QUALITÉ DES DONNÉES – PARTIE 115 : DONNÉES PERMANENTES : ÉCHANGE DES IDENTIFICATEURS QUALITÉ : EXIGENCES SYNTAXIQUES, SÉMANTIQUES ET DE RÉSOLUTION
ISO 8000-116	QUALITÉ DES DONNÉES – PARTIE 116 : DONNÉES PERMANENTES : ÉCHANGE DES IDENTIFICATEURS QUALITÉ : APPLICATION DE L'ISO 8000-115 À LA MISE EN FORME DES IDENTIFICATEURS OFFICIELS D'ENTITÉS JURIDIQUES
ISO 8000-120	Qualité des données – Partie 120 : Données permanentes : Échange des données caractéristiques : Provenance
ISO 8000-130	QUALITÉ DES DONNÉES – PARTIE 130 : DONNÉES PERMANENTES : ÉCHANGE DE DONNÉES CARACTÉRISTIQUES : EXACTITUDE
ISO 8000-140	QUALITÉ DES DONNÉES – PARTIE 140 : DONNÉES PERMANENTES : ÉCHANGE DE DONNÉES CARACTÉRISTIQUES : COMPLÉTUDE

ISO 8000-2	QUALITÉ DES DONNÉES – PARTIE 2 : VOCABULAIRE
ISO 8000-61	Qualité des données – Partie 61 : Gestion de la qualité des données : Modèle de référence des procédés
ISO 8000-62	QUALITÉ DES DONNÉES – PARTIE 62 : GESTION DE LA QUALITÉ DES DONNÉES : ÉVALUATION DE LA MATURITÉ ORGANISATIONNELLE DES PROCESSUS : APPLICATION DES NORMES RELATIVES À L'ÉVALUATION DES PROCESSUS
ISO 8000-63	QUALITÉ DES DONNÉES – PARTIE 63 : GESTION DE LA QUALITÉ DES DONNÉES : ÉVALUATION DU PROCESSUS
ISO 8000-8	QUALITÉ DES DONNÉES – PARTIE 8 : INFORMATIONS ET QUALITÉ DES DONNÉES : CONCEPTS ET MESURAGE
ISO TR 14873	INFORMATION ET DOCUMENTATION – STATISTIQUES ET INDICATEURS DE QUALITÉ POUR L'ARCHIVAGE DU WEB
ISO TS 8000-1	QUALITÉ DES DONNÉES – PARTIE 1 : APERÇU
ISO TS 8000-150	QUALITÉ DES DONNÉES – PARTIE 150 : DONNÉES PERMANENTES : CADRE DE MANAGEMENT DE LA QUALITÉ
ISO TS 8000-311	QUALITÉ DES DONNÉES – PARTIE 311 : DIRECTIVES POUR L'APPLICATION DE LA QUALITÉ DES DONNÉES DE PRODUIT POUR LES FORMES (PDQ-S)
ISO TS 8000-60	QUALITÉ DES DONNÉES – PARTIE 60 : GESTION DE LA QUALITÉ DES DONNÉES : APERÇU
ISO/IEC 25012	INGÉNIERIE DU LOGICIEL – EXIGENCES DE QUALITÉ ET ÉVALUATION DU PRODUIT LOGICIEL (SQUARE) – MODÈLE DE LA QUALITÉ DES DONNÉES
ISO/IEC 25020	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – EXIGENCES DE QUALITÉ DU PRODUIT LOGICIEL ET ÉVALUATION (SQUARE) – MODÈLE DE RÉFÉRENCE DE MESURE ET GUIDE
ISO/IEC 38505.2	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – PARTIE 2 : IMPLICATIONS DE L'ISO/IEC 38505-1 POUR LA GESTION DES DONNÉES
ISO/IEC TR 12382	INDEX PERMUTÉ DU VOCABULAIRE DES TECHNOLOGIES DE L'INFORMATION
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC/IEEE 24765	Ingénierie des systèmes et du logiciel – Vocabulaire
ISO/IEC/IEEE 26511	Ingénierie des systèmes et du logiciel – Exigences pour les gestionnaires de l'information pour les utilisateurs de systèmes, logiciels, et services
ISO/TS 14048-03	Management environnemental – Analyse du cycle de vie – Format de documentation de données
ISO/TS 8000-1	Qualité des données – Partie 1 : Aperçu
ISO/TS 8000-110	Qualité des données – Partie 110 : Données permanentes : Échange des données caractéristiques : Syntaxe, sémantique, encodage et conformité aux spécifications de données
ISO/TS 8000-150	Qualité des données – Partie 150 : Données permanentes : Cadre de management de la qualité
ISO/TS 8000-65	[Disponible uniquement en anglais]
ISO/TS 9002	SYSTÈMES DE MANAGEMENT DE LA QUALITÉ – LIGNES DIRECTRICES POUR L'APPLICATION DE L'ISO 9001:2015
ITU-T E.840	Cadre statistique applicable à la notation et au classement comparatifs de la qualité de fonctionnement de réseau de bout en bout

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail

CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 101:2019	Intelligence artificielle : Conception éthique et utilisation de systèmes de décision automatisés
CAN/CIOSC 103-1:2020	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
ISO 25000 series	[Disponible uniquement en anglais]
ISO 25012	INGÉNIERIE DU LOGICIEL – EXIGENCES DE QUALITÉ ET ÉVALUATION DU PRODUIT LOGICIEL (SQUARE) – MODÈLE DE LA QUALITÉ DES DONNÉES
ISO 8000 series	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	Cadre d'assurance de la qualité
n/a	Cadre d'assurance de la qualité
n/a	Trousse de la qualité des données
IEEE P2896	[Disponible uniquement en anglais]
IEEE P2957	[Disponible uniquement en anglais]
IEEE P2963	[Disponible uniquement en anglais]
IEEE P2975	[Disponible uniquement en anglais]
IEEE P3205	[Disponible uniquement en anglais]
IEEE P3803	[Disponible uniquement en anglais]

Groupe de travail 3 : Accès, diffusion et conservation

Question clé 19 gestion du consentement

ANSI AARST MS-QA	[Disponible uniquement en anglais]
BSI BS 10012	[Disponible uniquement en anglais]
BSI BS 8611	[Disponible uniquement en anglais]
BSI PAS 1192-5	[Disponible uniquement en anglais]
BSI PD CEN/TS 16685	Technologies de l'information – Notification d'identification par radiofréquence (RFID) : Signe informationnel et informations complémentaires exigibles lorsque des lecteurs RFID sont déployés
BSI PD CEN/TS 17288	[Disponible uniquement en anglais]
CEN EN 14484	Informatique de santé – Transfert international des données personnelles de santé couvertes par la directive européenne sur la protection des données personnelles – Politique de sécurité de haut niveau
CEN EN 14485	Informatique de santé – Guide pour manipuler des données personnelles de santé dans des applications internationales dans le contexte de la directive européenne sur la protection des données personnelles
CEN EN 14822-2	Informatique de la santé – Composants d'information d'usage général – Partie 2 : Informations non médicales

CEN EN 15224	Systèmes de management de la qualité – Application de l'EN ISO 9001:2015 aux soins de santé
CEN/TR 15300	Informatique de santé – Cadre pour modélisation formelle des politiques de sécurité dans le domaine de la santé
CEN/TR 16674	[Disponible uniquement en anglais]
CEN/TS 15480-4	Systèmes de cartes d'identification – Carte Européenne du Citoyen – Partie 4 : Recommandations pour l'émission, l'exploitation et l'utilisation de la Carte Européenne du Citoyen
CEN-EN 16571	Technologies de l'information – Processus d'évaluation d'impact sur la vie privée des applications RFID
CLSI HS1-A2	[Disponible uniquement en anglais]
CLSI QMS01-A4	[Disponible uniquement en anglais]
CLSI QMS22	[Disponible uniquement en anglais]
CSA CAN/CSA-C22.2 NO. 60950-23-07	Matériels de traitement de l'information – Sécurité – Partie 23 : Matériels de grande taille pour le stockage des données
CSA CAN/ CSA-Z900.2.1-17	Tissus destinés à la reproduction assistée
CSA CSA Z710:15	Activités du Bureau du registre de la nation métisse
CSA CSA-Q830-03	Code type sur la protection des renseignements personnels
CSA PLUS 8300-96	[Disponible uniquement en anglais]
CSA PLUS 8830-95	[Disponible uniquement en anglais]
CSA Z316.7-12	Établissements effectuant la collecte d'échantillons primaires et laboratoires d'analyses de biologie médicale – Sécurité du patient et qualité des soins – Exigences pour la collecte, le transport et la conservation des échantillons
CSA Z8000-18	Établissements de santé canadiens
DS DS/CWA 50487	[Disponible uniquement en anglais]
ETSI EG 202 487	[Disponible uniquement en anglais]
ETSI GS INS 009	[Disponible uniquement en anglais]
ETSI GS ISI 002	[Disponible uniquement en anglais]
ETSI GS ISI 005	[Disponible uniquement en anglais]
ETSI SR 003 680	[Disponible uniquement en anglais]
ETSI TR 102 688-8	[Disponible uniquement en anglais]
ETSI TR 102 935	[Disponible uniquement en anglais]
ETSI TR 103 304	[Disponible uniquement en anglais]
ETSI TR 103 603	[Disponible uniquement en anglais]
ETSI TR 103 644	[Disponible uniquement en anglais]
ETSI TR 118 516	[Disponible uniquement en anglais]
IEEE 1735	[Disponible uniquement en anglais]
ISO 10781	Informatique de santé – modèle fonctionnel d'un système de dossier de santé informatisé, publication 2 (EHR FM)
ISO 22600-3	INFORMATIQUE DE SANTÉ – GESTION DE PRIVILÈGES ET CONTRÔLE D'ACCÈS – PARTIE 3 : MISES EN OEUVRE
ISO 22857	Informatique de santé – Lignes directrices sur la protection des données pour faciliter les flux d'information sur la santé du personnel de part et d'autre des frontières
ISO 5127	INFORMATION ET DOCUMENTATION – FONDATIONS ET VOCABULAIRE
ISO 8000-100	Qualité des données – Partie 100 : Données permanentes : Échange des données caractéristiques : Aperçu général

ISO 8000-120	QUALITÉ DES DONNÉES – PARTIE 120 : DONNÉES PERMANENTES : ÉCHANGE DES DONNÉES CARACTÉRISTIQUES : PROVENANCE
ISO 8000-130	QUALITÉ DES DONNÉES – PARTIE 130 : DONNÉES PERMANENTES : ÉCHANGE DE DONNÉES CARACTÉRISTIQUES : EXACTITUDE
ISO 8000-140	QUALITÉ DES DONNÉES – PARTIE 140 : DONNÉES PERMANENTES : ÉCHANGE DE DONNÉES CARACTÉRISTIQUES : COMPLÉTUDE
ISO 8000-61	Qualité des données – Partie 61 : Gestion de la qualité des données : Modèle de référence des procédés
ISO 834-2	ESSAIS DE RÉSISTANCE AU FEU – ÉLÉMENTS DE CONSTRUCTION – PARTIE 2 : TITRE MANQUE
ISO HL7 21731	INFORMATIQUE DE SANTÉ – HL7 VERSION 3 – MODÈLE D'INFORMATION DE RÉFÉRENCE – VERSION 1
ISO TR 11636	INFORMATIQUE DE SANTÉ – RÉSEAU PRIVÉ, VIRTUEL, DYNAMIQUE, SUR DEMANDE POUR INFRASTRUCTURE D'INFORMATION DE SANTÉ
ISO TS 20658	LABORATOIRES DE BIOLOGIE MÉDICALE – EXIGENCES POUR LE PRÉLÈVEMENT, LE TRANSPORT, LA RÉCEPTION ET LA MANIPULATION DES ÉCHANTILLONS
ISO TS 27790	INFORMATIQUE DE SANTÉ – CADRE D'ENREGISTREMENT DE DOCUMENT
ISO TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ISO TS 8000-150	QUALITÉ DES DONNÉES – PARTIE 150 : DONNÉES PERMANENTES : CADRE DE MANAGEMENT DE LA QUALITÉ
ISO/IEC 10181-3	TECHNOLOGIES DE L'INFORMATION – INTERCONNEXION DE SYSTÈMES OUVERTS (OSI) – CADRES DE SÉCURITÉ POUR LES SYSTÈMES OUVERTS : CADRE DE CONTRÔLE D'ACCÈS
ISO/IEC 10746-2	TECHNOLOGIES DE L'INFORMATION – TRAITEMENT RÉPARTI OUVERT – MODÈLE DE RÉFÉRENCE : FONDEMENTS – PARTIE 2 :
ISO/IEC 10779	TECHNOLOGIES DE L'INFORMATION – LIGNES DIRECTRICES POUR L'ACCESSIBILITÉ AUX ÉQUIPEMENTS DE BUREAU PAR LES PERSONNES ÂGÉES ET LES PERSONNES HANDICAPÉES
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 24745	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – PROTECTION DES INFORMATIONS BIOMÉTRIQUES
ISO/IEC 29100	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CADRE PRIVÉ – AMENDEMENT 1 : CLARIFICATIONS
ISO/IEC 29101	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – ARCHITECTURE DE RÉFÉRENCE DE LA PROTECTION DE LA VIE PRIVÉE
ISO/IEC 29134	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR L'ÉTUDE D'IMPACTS SUR LA VIE PRIVÉE
ISO/IEC 29146	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CADRE POUR GESTION D'ACCÈS
ISO/IEC 29187-1	TECHNOLOGIES DE L'INFORMATION – IDENTIFICATION DES EXIGENCES DE PROTECTION PRIVÉE CONCERNANT L'APPRENTISSAGE, L'ÉDUCATION ET LA FORMATION (AÉF) – PARTIE 1 : CADRE GÉNÉRAL ET MODÈLE DE RÉFÉRENCE
ISO/IEC 29190:18	[Disponible uniquement en anglais]
ISO/IEC TR 23186:20	[Disponible uniquement en anglais]
ISO/IEC TR 24714-1	TECHNOLOGIES DE L'INFORMATION – BIOMÉTRIE – CONSIDÉRATIONS JURIDICTIONNELLES ET SOCIÉTALES POUR APPLICATIONS COMMERCIALES – PARTIE 1 : GUIDAGE GÉNÉRAL
ISO/IEC TR 24729-4	TECHNOLOGIES DE L'INFORMATION – IDENTIFICATION DE RADIOFRÉQUENCES POUR LA GESTION D'ITEMS – LIGNES DIRECTRICES POUR LA MISE EN OEUVRE – PARTIE 4 : SÉCURITÉ DES DONNÉES DE REPÈRE

ISO/IEC TR 24772	TECHNOLOGIES DE L'INFORMATION – LANGAGES DE PROGRAMMATION – CONDUITE POUR ÉVITER LES VULNÉRABILITÉS DANS LES LANGAGES DE PROGRAMMATION À TRAVERS LA SÉLECTION ET L'USAGE DE LA LANGUE
ISO/TR 17791	INFORMATIQUE DE LA SANTÉ – CONSEILS SUR LES NORMES DE SÉCURITÉ DES LOGICIELS DE LA SANTÉ
ISO/TR 21548	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Lignes directrices
ISO/TR 22221	Informatique de santé – Principes et indications d'exploitation d'un entrepôt de données cliniques
ISO/TS 14265	Informatique de santé – Classification des besoins pour le traitement des informations de santé personnelles
ISO/TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO/TS 19475-2	Gestion de documents – Exigences minimales pour le stockage des documents – Partie 2 : Stockage
ISO/TS 20658	Laboratoires de biologie médicale – Exigences pour le prélèvement, le transport, la réception et la manipulation des échantillons
ISO/TS 21547	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Principes
ISO/TS 22600-3	INFORMATIQUE DE SANTÉ – GESTION DE PRIVILÈGES ET CONTRÔLE D'ACCÈS – PARTIE 3 : MISES EN OEUVRE
ISO/TS 27790	Informatique de santé – Cadre d'enregistrement de document
ISO/TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO/WD 24366	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 103-1:2020	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
IEEE P7002	[Disponible uniquement en anglais]
IEEE P7004	[Disponible uniquement en anglais]
IEEE P7005	[Disponible uniquement en anglais]
IEEE P7006	[Disponible uniquement en anglais]
IEEE P7008	[Disponible uniquement en anglais]
IEEE P7012	[Disponible uniquement en anglais]
IEEE P7014	[Disponible uniquement en anglais]
IEEE P2089	[Disponible uniquement en anglais]
IEEE P3800	[Disponible uniquement en anglais]
IEEE P2895	[Disponible uniquement en anglais]
IEEE IC16-002	[Disponible uniquement en anglais]
IEEE IC17-002	[Disponible uniquement en anglais]
IEEE IC19-004	[Disponible uniquement en anglais]
IEEE IC18-004	[Disponible uniquement en anglais]

Question clé 20
accès aux données

BSI BS 10102-2	[Disponible uniquement en anglais]
ISO 23081-2	INFORMATION ET DOCUMENTATION – GESTION DES MÉTADONNÉES POUR L'INFORMATION ET LES DOCUMENTS – PARTIE 2 : CONCEPTS ET MISE EN OEUVRE
ISO/IEC 13522-6	TECHNOLOGIES DE L'INFORMATION – CODAGE DE L'INFORMATION MULTIMÉDIA ET HYPERMÉDIA – PARTIE 6 : SUPPORT POUR LES APPLICATIONS INTERACTIVES AMÉLIORÉES
ISO/IEC 27002	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CODE DE BONNE PRATIQUE POUR LE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION
ISO/IEC 27040	TECHNOLOGIE DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE STOCKAGE
ISO/IEC 27050-1	TECHNOLOGIES DE L'INFORMATION – DÉCOUVERTE ÉLECTRONIQUE – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 29146	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CADRE POUR GESTION D'ACCÈS
ISO/IEC TR 30166	L'internet des objets (IoT) – L'internet industriel des objets
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC/IEEE 24765	Ingénierie des systèmes et du logiciel – Vocabulaire
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-8	Gouvernance des données-Partie 8 : Cadre de géorésidence et de souveraineté
IEEE P2975	[Disponible uniquement en anglais]
CSA Z8003	Recherche et évaluation de la conception des établissements de soins de santé

Question clé 21
conservation de données

ANSI INCITS 306	[Disponible uniquement en anglais]
ANSI INCITS 516	[Disponible uniquement en anglais]
ANSI X9.129	[Disponible uniquement en anglais]
ANSI X9.84	[Disponible uniquement en anglais]
BSI BS 10008-2	[Disponible uniquement en anglais]
BSI BS 10012 + A1	[Disponible uniquement en anglais]
BSI BS 10102-1	[Disponible uniquement en anglais]
BSI PAS 183	[Disponible uniquement en anglais]
BSI PAS 1885	[Disponible uniquement en anglais]
CEN EN 14484	Informatique de santé – Transfert international des données personelles de santé couvertes par la directive européenne sur la protection des données personelles – Politique de sécurité de haut niveau

CEN EN 14485	Informatique de santé – Guide pour manipuler des données personnelles de santé dans des applications internationales dans le contexte de la directive européenne sur la protection des données personnelles
CEN EN 16072	Systèmes de transport intelligents – ESafety – Exigences opérationnelles du service eCall paneuropéen
CEN EN 16571	Technologies de l'information – Processus d'évaluation d'impact sur la vie privée des applications RFID
CEN/TR 16673	[Disponible uniquement en anglais]
CEN/TR 16674	[Disponible uniquement en anglais]
CEN/TR 16742	Systèmes de transport intelligents – Aspects de la vie privée dans les normes et les systèmes en Europe
CEN/TS 15480-4	Systèmes de cartes d'identification – Carte Européenne du Citoyen – Partie 4 : Recommandations pour l'émission, l'exploitation et l'utilisation de la Carte Européenne du Citoyen
CENELEC CEN/CLC/ ETSI/TR 50572	[Disponible uniquement en anglais]
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN SPEC 91357	[Disponible uniquement en anglais]
DS DS/CWA 17356	[Disponible uniquement en anglais]
ETSI EG 202 798	[Disponible uniquement en anglais]
ETSI ETR 295	[Disponible uniquement en anglais]
ETSI GS INS 009	[Disponible uniquement en anglais]
ETSI GS ISI 008	[Disponible uniquement en anglais]
ETSI GS MOI 002	[Disponible uniquement en anglais]
ETSI GS MOI 003	[Disponible uniquement en anglais]
ETSI GS MOI 010	[Disponible uniquement en anglais]
ETSI GS NFV-SEC 006	[Disponible uniquement en anglais]
ETSI GS NGP 001	[Disponible uniquement en anglais]
ETSI SR 002 298	[Disponible uniquement en anglais]
ETSI SR 002 564	[Disponible uniquement en anglais]
ETSI SR 003 392	[Disponible uniquement en anglais]
ETSI TR 102 299	[Disponible uniquement en anglais]
ETSI TR 102 438	[Disponible uniquement en anglais]
ETSI TR 102 512	[Disponible uniquement en anglais]
ETSI TR 102 725	[Disponible uniquement en anglais]
ETSI TR 102 762	[Disponible uniquement en anglais]
ETSI TR 103 118	[Disponible uniquement en anglais]
ETSI TR 103 304	[Disponible uniquement en anglais]
ETSI TR 103 305-5	[Disponible uniquement en anglais]
ETSI TR 103 370	[Disponible uniquement en anglais]
ETSI TR 103 533	[Disponible uniquement en anglais]
ETSI TR 103 534-2	[Disponible uniquement en anglais]
ETSI TR 103 591	[Disponible uniquement en anglais]
ETSI TR 103 603	[Disponible uniquement en anglais]
ETSI TS 102 412	[Disponible uniquement en anglais]

ETSI TS 102 657	[Disponible uniquement en anglais]
ETSI TS 103 443-2	[Disponible uniquement en anglais]
ETSI TS 103 443-3	[Disponible uniquement en anglais]
ETSI TS 103 443-5	[Disponible uniquement en anglais]
ETSI TS 103 443-6	[Disponible uniquement en anglais]
ETSI TS 105 174-2	[Disponible uniquement en anglais]
ETSI TS 118 103	[Disponible uniquement en anglais]
IEC 61360-4	[Disponible uniquement en anglais]
IEC 61512-4	Contrôle-commande des processus de fabrication par lots – Partie 4 : Enregistrements de production par lots
IEC 63119-1	Échange d'informations pour le service d'itinérance de la recharge des véhicules électriques – Partie 1 : Généralités
IEC 82304-1	Logiciels de santé – Partie 1 : Exigences générales pour la sécurité des produits
IEC TR 80001-2-8	[Disponible uniquement en anglais]
IEC/TR 62939-1	[Disponible uniquement en anglais]
IEC/TR 80001-2-8	[Disponible uniquement en anglais]
IEEE 2001	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
IEEE 2755.1	[Disponible uniquement en anglais]
ISO/IEC 15944-9	Technologies de l'information – Vue opérationnelle des affaires – Partie 9 : Cadre de traçabilité des transactions d'affaires pour l'échange d'engagements
ISO/IEC 17789	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – ARCHITECTURE DE RÉFÉRENCE
ISO/IEC 17789:16	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – ARCHITECTURE DE RÉFÉRENCE
ISO/IEC 18014-4	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SERVICES D'HORODATAGE – PARTIE 4 : TRAÇABILITÉ DES SOURCES DU TEMPS
ISO/IEC 18043	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉLECTION, DÉPLOIEMENT ET OPÉRATIONS DES SYSTÈMES DE DÉTECTION D'INTRUSION
ISO/IEC 19086-1	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 19086-3	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 3 : EXIGENCES DE CONFORMITÉ ESSENTIELLES
ISO/IEC 19086-4	INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 4 : ELÉMENTS DE SÉCURITÉ ET DE PROTECTION DES PII
ISO/IEC 19286	CARTES D'IDENTIFICATION – CARTES À CIRCUIT INTÉGRÉ – PROTOCOLES ET SERVICES RENFORÇANT LA PROTECTION DES DONNÉES PERSONNELLES
ISO/IEC 19941	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – INTEROPÉRABILITÉ ET PORTABILITÉ
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO/IEC 20748.2	TECHNOLOGIES DE L'INFORMATION – ÉDUCATION, FORMATION ET APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 2 : EXIGENCES RELATIVES AU SYSTÈME
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 27004	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION – SURVEILLANCE, MESURAGE, ANALYSE ET ÉVALUATION
ISO/IEC 27034-5	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SECURITE – SECURITE DES APPLICATIONS – PARTIE 5 : PROTOCOLES ET STRUCTURE DE DONNÉES DE CONTRÔLES DE SÉCURITÉ D'APPLICATION

ISO/IEC 27037	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR L'IDENTIFICATION, LA COLLECTE, L'ACQUISITION ET LA PRÉSERVATION DE PREUVES NUMÉRIQUES
ISO/IEC 27039	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉLECTION, DÉPLOIEMENT ET OPÉRATIONS DES SYSTÈMES DE DÉTECTION ET PRÉVENTION D'INTRUSION
ISO/IEC 27040	TECHNOLOGIE DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE STOCKAGE
ISO/IEC 27050-1	TECHNOLOGIES DE L'INFORMATION – DÉCOUVERTE ÉLECTRONIQUE – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 29100	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CADRE PRIVÉ – AMENDEMENT 1 : CLARIFICATIONS
ISO/IEC 29101	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – ARCHITECTURE DE RÉFÉRENCE DE LA PROTECTION DE LA VIE PRIVÉE
ISO/IEC 29110-4-3	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – PROFILS DE CYCLE DE VIE POUR TRÈS PETITS ORGANISMES (TPO) – PARTIE 4-3 : PRESTATION DE SERVICES – SPÉCIFICATION DE PROFIL
ISO/IEC 29134	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR L'ÉTUDE D'IMPACTS SUR LA VIE PRIVÉE
ISO/IEC 29151	Technologies de l'information – Techniques de sécurité – code de bonne pratique pour la protection des données à caractère personnel
ISO/IEC 29155-2	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – CADRE DE CONDUITE DE TESTS DE PERFORMANCE DE PROJET DE TECHNOLOGIES DE L'INFORMATION – PARTIE 2 : EXIGENCES POUR LE MARQUAGE DE RÉFÉRENCE
ISO/IEC 29184	TECHNOLOGIES DE L'INFORMATION – DÉCLARATIONS DE CONFIDENTIALITÉ EN LIGNE ET LES CONSENTEMENTS
ISO/IEC 29341-30-1	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE DISPOSITIF UPNP – PARTIE 30-1 : PROTOCOLE DE CONTRÔLE DE DISPOSITIF DE GESTION ET DE CONTRÔLE DE L'INTERNET DES OBJETS – APERÇU GÉNÉRAL DE L'ARCHITECTURE DE GESTION ET DE CONTRÔLE DE L'INTERNET DES OBJETS
ISO/IEC 30137-1	TECHNOLOGIES DE L'INFORMATION – UTILISATION DE LA BIOMÉTRIE DANS LES SYSTÈMES DE VIDÉOSURVEILLANCE – PARTIE 1 : CONCEPTION ET SPÉCIFICATION
ISO/IEC 38505-1	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données
ISO/IEC TR 15067-3-2	[Disponible uniquement en anglais]
ISO/IEC TR 15947	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CADRE DE DÉTECTION DE L'INTRUSION DANS LES SYSTÈMES DES TECHNOLOGIES DE L'INFORMATION
ISO/IEC TR 16166	TECHNOLOGIES DE L'INFORMATION – TÉLÉINFORMATIQUE – RÉSEAUX D'ENTREPRISE DE PROCHAINE GÉNÉRATION (NGCN) – SÉCURITÉ DES COMMUNICATIONS SUR LA BASE DE SESSIONS
ISO/IEC TR 20000-9	TECHNOLOGIES DE L'INFORMATION – GESTION DES SERVICES – PARTIE 9 : APPLICATION DE L'ISO/IEC 20000-1 AU SERVICES DE CLOUD
ISO/IEC TR 20748-2	TECHNOLOGIES DE L'INFORMATION – ÉDUCATION, FORMATION ET APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 2 : EXIGENCES RELATIVES AU SYSTÈME
ISO/IEC TR 24714-1	Technologies de l'information – Biométrie – Considérations juridictionnelles et sociétales pour applications commerciales – Partie 1 : Guidage général
ISO/IEC TR 27550	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – INGÉNIERIE DE LA VIE PRIVÉE POUR LES PROCESSUS DU CYCLE DE VIE DES SYSTÈMES
ISO/IEC TR 29110-5-3	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – PROFILS DE CYCLE DE VIE POUR TRÈS PETITS ORGANISMES (TPO) – PARTIE 5-3 : LIGNES DIRECTICES DE PRESTATION DES SERVICES
ISO/IEC TR 29196	TECHNOLOGIES DE L'INFORMATION – DIRECTIVES POUR L'INSCRIPTION BIOMÉTRIQUE
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC TS 27034-5-1	INFORMATION TECHNOLOGY – APPLICATION SECURITY – PART 5-1 : PROTOCOLS AND APPLICATION SECURITY CONTROLS DATA STRUCTURE, XML SCHEMAS

ISO/IEC/IEEE 12207	SYSTEMS AND SOFTWARE ENGINEERING – SOFTWARE LIFE CYCLE PROCESSES
ISO/IEC/IEEE 15289	SYSTEMS AND SOFTWARE ENGINEERING – CONTENT OF LIFE-CYCLE INFORMATION ITEMS (DOCUMENTATION)
ISO/IEC/IEEE 23026	Ingénierie des systèmes et du logiciel – Ingénierie et gestion de sites web pour les systèmes, logiciels et services d'information
ISO/IEC/IEEE 24765	Ingénierie des systèmes et du logiciel – Vocabulaire
ISO/IEC/IEEE 29148	Ingénierie des systèmes et du logiciel – Processus du cycle de vie – Ingénierie des exigences
ISO/IEC/IEEE 90003	INGÉNIERIE DU LOGICIEL – LIGNES DIRECTRICES POUR L'APPLICATION DE L'ISO 9001:2015 AUX LOGICIELS INFORMATIQUES
ISO/TR 10255	Applications de la gestion des documents – Technologie de stockage sur disque optique, gestion et normes
ISO/TR 12859	Systèmes intelligents de transport – Architecture de système – Aspects privés dans les normes et les systèmes SIT
ISO/TR 14742	Services financiers – Recommandations sur les algorithmes cryptographiques et leur utilisation
ISO/TR 17427-3	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 3 : Concept des opérations (ConOps) pour les systèmes 'principaux'
ISO/TR 17427-4	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 4 : Exigences minimales du système et comportement des systèmes principaux
ISO/TR 17427-7	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 7 : Aspects relatifs à la vie privée
ISO/TR 17797	ARCHIVAGE ÉLECTRONIQUE – SÉLECTION D'UN SUPPORT DE STOCKAGE NUMÉRIQUE POUR UNE PRÉSERVATION À LONG TERME
ISO/TR 80002-2	LOGICIELS DE DISPOSITIFS MÉDICAUX – PARTIE 2 : VALIDATION DES LOGICIELS POUR LES SYSTÈMES DE QUALITÉ DES DISPOSITIFS MÉDICAUX
ISO/TS 17427	Systèmes intelligents de transport – Systèmes coopératifs – Rôles et responsabilités dans le contexte des ITS fondés sur l'architecture de systèmes coopératifs
ISO/TS 19299	Perception de télépéage – Cadre de sécurité
ISO/TS 21089	INFORMATIQUE DE SANTÉ – FLUX D'INFORMATIONS "TRUSTED END-TO-END"
ISO/TS 26683-1	Systèmes intelligents de transport – Identification et communication du contenu des marchandises transportées par voie terrestre – Partie 1 : Contexte, architecture et normes référencées
ITU-T L.1300	Bonnes pratiques pour les centres de traitement de données écologiques
ITU-T L.64	Exigences relatives aux étiquettes ID pour la gestion de l'infrastructure et des éléments de réseau
ITU-T M.3363	Exigences pour la gestion des données dans le réseau de gestion des télécommunications
ITU-T SERIES D SUPP 4	[Disponible uniquement en anglais]
ITU-T SERIES X SUPP 13	[Disponible uniquement en anglais]
ITU-T SERIES X SUPP 32	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 40	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 55	[Disponible uniquement en anglais]
ITU-T X.1058	[Disponible uniquement en anglais]
ITU-T X.1147	Exigences de sécurité et cadre pour l'analyse des mégadonnées dans les services Internet sur mobile
ITU-T X.1250	Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité
ITU-T X.1601	Cadre de sécurité applicable à l'informatique en nuage
ITU-T X.1602	[Disponible uniquement en anglais]
ITU-T X.1603	[Disponible uniquement en anglais]
ITU-T X.1642	[Disponible uniquement en anglais]

ITU-T Y.3174	Cadre pour le traitement des données en vue de permettre la mise en œuvre de l'apprentissage automatique dans les réseaux futurs, y compris les IMT-2020
ITU-T Y.3502	Technologies de l'information – Informatique en nuage – Architecture de référence
ITU-T Y.3519	Informatique en nuage – Architecture fonctionnelle des mégadonnées en tant que service
ITU-T Y.3600	Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage
ITU-T Y.3601	Mégadonnées – Cadre et exigences pour l'échange de données
ITU-T Y.3602	Mégadonnées – Exigences fonctionnelles relatives à la provenance des données
ITU-T Y.3604	Mégadonnées – Aperçu de la préservation des données et exigences
ITU-T Y.4556	Exigences et architecture fonctionnelle d'une communauté résidentielle intelligente
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des donnée
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 104	Contrôles de cybersécurité de base pour les petites et moyennes organisations
IEEE 1619-2018	[Disponible uniquement en anglais]

Question clé 22
gestion des identités – validation et authentification (personnes, entités et appareils)

ANSI INCITS 501	[Disponible uniquement en anglais]
ANSI INCITS 504-1	[Disponible uniquement en anglais]
ANSI X9 TR-48	[Disponible uniquement en anglais]
ANSI X9.111	[Disponible uniquement en anglais]
ANSI X9.73	[Disponible uniquement en anglais]
ANSI X9.84	[Disponible uniquement en anglais]
BSI PAS 11281	[Disponible uniquement en anglais]
BSI PAS 1296	[Disponible uniquement en anglais]
BSI PAS 499	[Disponible uniquement en anglais]
BSI PAS 96	[Disponible uniquement en anglais]
CEN 12830	Enregistreurs de température pour le transport, le stockage et la distribution des marchandises thermosensibles – Essais, performance, aptitude à l'emploi
CEN 16495	Gestion du trafic aérien – Sécurité de l'information pour les organismes assurant le soutien des opérations de l'aviation civile
CEN 419221-5	Profils de protection pour les modules cryptographiques de prestataires de services de confiance – Partie 5 : Module cryptographique pour les services de confiance
CEN EN 12896-5	Transports publics – Modèle de données de référence – Partie 5 : gestion tarifaire
CEN/TS 16614-3	[Disponible uniquement en anglais]
DIN CEN/TS 16614-3	Transport Public – Échanges des informations planifiées (NeTEx) – Partie 3 : Échange des informations tarifaires pour le transport public
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN SPEC 91347	[Disponible uniquement en anglais]

DS DS/CWA 17302	[Disponible uniquement en anglais]
ETSI EN 319 411-1	[Disponible uniquement en anglais]
ETSI EN 319 521	[Disponible uniquement en anglais]
ETSI EN 319 522-2	[Disponible uniquement en anglais]
ETSI EN 319 522-3	[Disponible uniquement en anglais]
ETSI EN 319 522-4-3	[Disponible uniquement en anglais]
ETSI EN 319 532-3 V1.2.1	[Disponible uniquement en anglais]
ETSI GR PDL 001	[Disponible uniquement en anglais]
ETSI GS ISI 002	[Disponible uniquement en anglais]
ETSI GS NFV-SEC 006	[Disponible uniquement en anglais]
ETSI GS NFV-SEC 014	[Disponible uniquement en anglais]
ETSI SR 003 186	[Disponible uniquement en anglais]
ETSI SR 003 391	[Disponible uniquement en anglais]
ETSI SR 019 050	[Disponible uniquement en anglais]
ETSI TR 103 303	[Disponible uniquement en anglais]
ETSI TR 103 305-1	[Disponible uniquement en anglais]
ETSI TR 103 305-5	[Disponible uniquement en anglais]
ETSI TR 103 604	[Disponible uniquement en anglais]
ETSI TR 103 644	[Disponible uniquement en anglais]
ETSI TR 103 684	[Disponible uniquement en anglais]
ETSI TR 119 530	[Disponible uniquement en anglais]
ETSI TS 101 553-2	[Disponible uniquement en anglais]
ETSI TS 102 412	[Disponible uniquement en anglais]
ETSI TS 103 436	[Disponible uniquement en anglais]
ETSI TS 103 458	[Disponible uniquement en anglais]
ETSI TS 103 645	[Disponible uniquement en anglais]
ETSI TS 118 103	[Disponible uniquement en anglais]
ETSI TS 119 102-2	[Disponible uniquement en anglais]
ETSI TS 119 403-3	[Disponible uniquement en anglais]
ETSI TS 119 432	[Disponible uniquement en anglais]
ETSI TS 119 512	[Disponible uniquement en anglais]
ETSI TS 119 524-1	[Disponible uniquement en anglais]
ETSI TS 119 534-1	[Disponible uniquement en anglais]
ETSI TS 119 612	[Disponible uniquement en anglais]
ETSI TS 133 107	[Disponible uniquement en anglais]
ETSI TS 133 180	[Disponible uniquement en anglais]
ETSI TS 133 401	[Disponible uniquement en anglais]
ETSI TS 133 501	[Disponible uniquement en anglais]
IEC 60050-741	Vocabulaire Électrotechnique International (IEV) – Partie 741 : Internet des Objets (IdO)
IEC 60839-5-3	Systèmes d'alarme et de sécurité électroniques – Partie 5-3 : Systèmes de transmission d'alarme – Exigences pour les transmetteurs du centre de réception (RCT)

IEC 62443-2-4	Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4 : Exigences de programme de sécurité pour les fournisseurs de service IACS
IEC TR 62559-1	Méthodologie des cas d'utilisation – Partie 1 : Concept et processus de normalisation
IEEE 1865	[Disponible uniquement en anglais]
IEEE 1865.2	[Disponible uniquement en anglais]
IEEE 1934	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
IEEE 802.1CF	[Disponible uniquement en anglais]
IEEE 802.1X	[Disponible uniquement en anglais]
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	[Disponible uniquement en anglais]
IEEE WHITE PAPER-0	[Disponible uniquement en anglais]
ISO 12812-1	OPÉRATIONS BANCAIRES DE BASE – SERVICES FINANCIERS MOBILES – PARTIE 1 : CADRE GÉNÉRAL
ISO 14721	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – SYSTÈME OUVERT D'ARCHIVAGE D'INFORMATION (SOAI) – MODÈLE DE RÉFÉRENCE
ISO 15118-1	VÉHICULES ROUTIERS – INTERFACE DE COMMUNICATION ENTRE VÉHICULE ET RÉSEAU ÉLECTRIQUE – PARTIE 1 : INFORMATIONS GÉNÉRALES ET DÉFINITION DE CAS D'UTILISATION
ISO 16484-5	SYSTÈMES D'AUTOMATISATION ET DE GESTION TECHNIQUE DU BÂTIMENT – PARTIE 5 : PROTOCOLE DE COMMUNICATION DE DONNÉES
ISO 20700	LIGNES DIRECTRICES RELATIVES AUX SERVICES DE CONSEIL EN MANAGEMENT
ISO 22300	SÉCURITÉ ET RÉSILIENCE – VOCABULAIRE
ISO 9564-4	SERCICES FINANCIERS – GESTION ET SÉCURITÉ DU NUMÉRO PERSONNEL D'IDENTIFICATION (PIN) – PARTIE 4 : EXIGENCES POUR LA MANIPULATION PIN DANS LE COMMERCE ÉLECTRONIQUE POUR LES TRANSACTIONS DE PAIEMENT
ISO TS 11633-1	INFORMATIQUE DE SANTÉ – MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION POUR LA MAINTENANCE À DISTANCE DES DISPOSITIFS MÉDICAUX ET DES SYSTÈMES D'INFORMATION MÉDICALE – PARTIE 1 : EXIGENCES ET ANALYSE DU RISQUE
ISO TS 12812-5	OPÉRATIONS BANCAIRES DE BASE – SERVICES FINANCIERS MOBILES – PARTIE 5 : PAIEMENTS MOBILES À ENTREPRISES
ISO TS 23029	[Disponible uniquement en anglais]
ISO/IEC 14776-454	[Disponible uniquement en anglais]
ISO/IEC 14776-481	[Disponible uniquement en anglais]
ISO/IEC 18013-1	TECHNOLOGIES DE L'INFORMATION – IDENTIFICATION DES PERSONNES – PERMIS DE CONDUIRE CONFORME À L'ISO – PARTIE 1 : CARACTÉRISTIQUES PHYSIQUES ET JEU DE DONNÉES DE BASE
ISO/IEC 18028-4	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE RÉSEAUX TI – PARTIE 4 : TÉLÉACCÈS DE LA SÉCURITÉ
ISO/IEC 18370-2	TECHNOLOGIE DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SIGNATURES NUMÉRIQUES EN AVEUGLE – PARTIE 2 : MÉCANISMES FONDÉS SUR LE LOGARITHME DISCRET
ISO/IEC 19086-4	INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 4 : ELÉMENTS DE SÉCURITÉ ET DE PROTECTION DES PII
ISO/IEC 19286	CARTES D'IDENTIFICATION – CARTES À CIRCUIT INTÉGRÉ – PROTOCOLES ET SERVICES RENFORÇANT LA PROTECTION DES DONNÉES PERSONNELLES
ISO/IEC 19941	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – INTEROPÉRABILITÉ ET PORTABILITÉ
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE

ISO/IEC 20248	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES D'IDENTIFICATION AUTOMATIQUE ET DE CAPTURE DE DONNÉES – STRUCTURES DE DONNÉES – MÉTA-STRUCTURE DE SIGNATURE NUMÉRIQUE
ISO/IEC 20924	TECHNOLOGIES DE L'INFORMATION – INTERNET DES OBJETS (IDO) – VOCABULAIRE
ISO/IEC 21878	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR LA CONCEPTION ET L'IMPLÉMENTATION SÉCURISÉES DES SERVEURS VIRTUALISÉS
ISO/IEC 23006-3	TECHNOLOGIES DE L'INFORMATION – TECHNOLOGIES DE LA PLATE-FORME DE SERVICES MULTIMÉDIA – PARTIE 3 : CONFORMITÉ ET LOGICIEL DE RÉFÉRENCE
ISO/IEC 24759	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – EXIGENCES D'ESSAI POUR MODULES CRYPTOGRAPHIQUES
ISO/IEC 24760-1	SÉCURITÉ IT ET CONFIDENTIALITÉ – CADRE POUR LA GESTION DE L'IDENTITÉ – PARTIE 1 : TERMINOLOGIE ET CONCEPTS
ISO/IEC 24760-3	Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 3 : Mise en œuvre
ISO/IEC 25023	INGÉNIERIE DES SYSTÈMES ET DU LOGICIEL – EXIGENCES DE QUALITÉ ET ÉVALUATION DES SYSTÈMES ET DU LOGICIEL (SQUARE) – MESURAGE DE LA QUALITÉ DU PRODUIT LOGICIEL ET DU SYSTÈME
ISO/IEC 27019	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – MESURES DE SÉCURITÉ DE L'INFORMATION POUR L'INDUSTRIE DES OPÉRATEURS DE L'ÉNERGIE
ISO/IEC 27021	TECHNOLOGIES DE L'INFORMATION – TECNIQUES DE SÉCURITÉ – EXIGENCES DE COMPÉTENCE POUR LES PROFESSIONNELS DE LA GESTION DES SYSTÈMES DE MANAGEMENT DE LA SÉCURITÉ
ISO/IEC 27036-4	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ D'INFORMATION POUR LA RELATION AVEC LE FOURNISSEUR – PARTIE 4 : LIGNES DIRECTRICES POUR LA SÉCURITÉ DES SERVICES DU NUAGE
ISO/IEC 30107-1	TECHNOLOGIES DE L'INFORMATION – DÉTECTION D'ATTAQUE DE PRÉSENTATION EN BIOMÉTRIE – PARTIE 1 : STRUCTURE
ISO/IEC 30118-2	TECHNOLOGIES DE L'INFORMATION – SPÉCIFICATION DE LA FONDATION POUR LA CONNECTIVITÉ OUVERTE (FONDATION OCF) – PARTIE 2 : SPÉCIFICATION DE SÉCURITÉ
ISO/IEC TR 20547-2	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 2 : CAS PRATIQUES ET EXIGENCES DÉRIVÉES
ISO/IEC TR 23188	[Disponible uniquement en anglais]
ISO/IEC TR 29156	TECHNOLOGIES DE L'INFORMATION – DIRECTIVES SPÉCIFIANT LES EXIGENCES DE PERFORMANCE AFIN D'ATTEINDRE LA SÉCURITÉ ET LES BESOINS D'UTILISATION DANS LES APPLICATIONS BIOMÉTRIQUES
ISO/IEC TR 30125	TECHNOLOGIES DE L'INFORMATION – BIOMÉTRIE UTILISÉE AVEC DES APPAREILS MOBILES
ISO/IEC TS 20540	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – TEST DE MODULES CRYPTOGRAPHIQUES DANS LEUR ENVIRONNEMENT D'EXPLOITATION
ISO/IEC TS 27008	INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – GUIDELINES FOR THE ASSESSMENT OF INFORMATION SECURITY CONTROLS
ISO/IEC/IEEE 8802-21	Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Exigences spécifiques – Partie 21 : Cadre des services indépendants des supports
ISO/IEC/IEEE 8802-21-1	Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Partie 21-1 : Services indépendants des supports
ISO/TR 20526	RAPPORT DE L'ÉTAT DE LA TECHNIQUE CONCERNANT LA BILLETTIQUE CENTRÉE SUR LE COMPTE USAGER
ISO/TS 11633-1	INFORMATIQUE DE SANTÉ – MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION POUR LA MAINTENANCE À DISTANCE DES DISPOSITIFS MÉDICAUX ET DES SYSTÈMES D'INFORMATION MÉDICALE – PARTIE 1 : EXIGENCES ET ANALYSE DU RISQUE
ISO/TS 12812-5	Opérations bancaires de base – Services financiers mobiles – Partie 5 : Paiements mobiles à entreprises

ISO/TS 23029	[Disponible uniquement en anglais]
ITU-T G.7701	Aspects communs de commande
ITU-T H.550	Architecture et entités fonctionnelles des plates-formes de passerelle de véhicule
ITU-T J.1	Transmission télévisuelle et sonore et réseaux câblés intégrés large bande : termes, définitions et acronymes
ITU-T J.298	Exigences et spécifications techniques d'un boîtier-décodeur hybride de télévision par câble compatible avec le transport de télévision de Terre et par satellite
ITU-T P.1502	Méthodologie d'évaluation de la qualité d'expérience concernant les services financiers numériques
ITU-T SERIES F SUPP 3	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 49	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 53	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 56	[Disponible uniquement en anglais]
ITU-T X.1038	Exigences de sécurité et architecture de référence pour les réseaux pilotés par logiciel
ITU-T X.1039	Mesures de sécurité techniques pour la mise en oeuvre des dimensions de sécurité UIT-T X.805
ITU-T X.1087	Contremesures techniques et opérationnelles pour les applications de la télébiométrie utilisant des dispositifs mobiles
ITU-T X.1127	[Disponible uniquement en anglais]
ITU-T X.1146	Lignes directrices pour garantir la protection des services à valeur ajoutée fournis par les opérateurs de télécommunication
ITU-T X.1258	[Disponible uniquement en anglais]
ITU-T X.1276	Protocole d'amélioration de l'authentification et métadonnées – Version 1.0
ITU-T X.1277	Cadre d'authentification universelle
ITU-T X.1331	[Disponible uniquement en anglais]
ITU-T X.1450	Lignes directrices sur les mécanismes d'authentification hybride et de gestion de clés dans le modèle client-serveur
ITU-T X.1605	[Disponible uniquement en anglais]
ITU-T X.1631	Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de sécurité de l'information fondés sur la norme ISO/CEI 27002 pour les services en nuage
ITU-T X.1642	[Disponible uniquement en anglais]
ITU-T Y.2342	Scénarios et exigences relatives aux capacités pour la chaîne de blocs pour l'évolution des réseaux de prochaine génération
ITU-T Y.4459	Cadre de l'architecture d'entité numérique pour l'interopérabilité dans l'Internet des objets
SAE J3101	[Disponible uniquement en anglais]
SAE PT-179	[Disponible uniquement en anglais]
SNZ AS/NZS 62676.1.1	[Disponible uniquement en anglais]
UL 827 BULLETIN	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO 17442:2019	SERVICES FINANCIERS – SCHÉMA D'IDENTIFIANT D'ENTITÉ LÉGALE (IEL)
ISO/CD 24366	[Disponible uniquement en anglais]
CAN/CIOSC 103-1	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
Pan-Canadian Trust Framework	Aperçu du cadre de confiance pancanadien : Une approche collaborative pour développer un cadre de confiance pancanadien
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données

CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 103-1:2020	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
CAN/CIOSC 103-3	Confiance et identité numérique – Partie 3 : Justificatifs d'identité numériques
CAN/CIOSC 103-4	Confiance et identité numérique – Partie 4 : Portefeuilles numériques
IEEE P1363.3/D9	[Disponible uniquement en anglais]
IEEE 802.1AR-2018	[Disponible uniquement en anglais]
IEEE 2410-2019	[Disponible uniquement en anglais]
DIACC PCTF 01	Pan-Canadian Trust Framework (PCTF) Model v1.0
DIACC PCTF 02	Pan-Canadian Trust Framework (PCTF) Notice & Consent : Component Overview and Conformance Profile v1.0
DIACC PCTF 03	Pan-Canadian Trust Framework (PCTF) Authentication : Component Overview and Conformance Profile v1.0
DIACC PCTF 04	Pan-Canadian Trust Framework (PCTF) Privacy : Component Overview and Conformance Profile v1.0
DIACC PCTF 05	Pan-Canadian Trust Framework (PCTF) Verified Person : Component Overview and Conformance Profile v1.0
DIACC PCTF 06	Pan-Canadian Trust Framework (PCTF) Verified Organization : Component Overview and Conformance Profile v1.0
DIACC PCTF 07	Pan-Canadian Trust Framework (PCTF) Credentials (Relationship & Attributes) : Component Overview and Conformance Profile v1.0
DIACC PCTF 08	Pan-Canadian Trust Framework (PCTF) Infrastructure (Technology & Operations) : Component Overview and Conformance Profile v1.0
DIACC PCTF 09	Pan-Canadian Trust Framework (PCTF) Assessment v1.0
DIACC PCTF 10	Pan-Canadian Trust Framework (PCTF) Glossary V1.0

Question clé 23
partage, échange, et intégration de données

ANSI INCITS 398	[Disponible uniquement en anglais]
ANSI INCITS 459	[Disponible uniquement en anglais]
ASTM E2468	[Disponible uniquement en anglais]
CEN EN 16570	Technologies de l'information – Notification d'identification par radiofréquence (RFID) – Signe informationnel et informations complémentaires devant être délivrées par les exploitants de systèmes d'application d'identification RFID
DIN 66398	[Disponible uniquement en anglais]
ISO 20614	INFORMATION ET DOCUMENTATION – PROTOCOLE D'ÉCHANGE DE DONNÉES POUR L'INTEROPÉRABILITÉ ET LA PRÉSERVATION
ISO/IEC 18598	[Disponible uniquement en anglais]
ISO/IEC 20889	TERMINOLOGIE ET CLASSIFICATION DES TECHNIQUES DE DÉ-IDENTIFICATION DE DONNÉES POUR LA PROTECTION DE LA VIE PRIVÉE
ISO/IEC 24713-3	TECHNOLOGIES DE L'INFORMATION – PROFILS BIOMÉTRIQUES POUR INTEROPÉRABILITÉ ET ÉCHANGE DE DONNÉES – PARTIE 3 : VÉRIFICATION BASÉE SUR LA BIOMÉTRIE ET IDENTIFICATION DES NAVIGATEURS
ISO/IEC 27701	TECHNIQUES DE SÉCURITÉ – EXTENSION D'ISO/IEC 27001 ET ISO/IEC 27002 AU MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE – EXIGENCES ET LIGNES DIRECTRICES

ISO/IEC TR 29144	TECHNOLOGIES DE L'INFORMATION – BIOMÉTRIQUE – UTILISATION DE LA TECHNOLOGIE BIOMÉTRIQUE DANS LES PROCESSUS ET LES APPLICATIONS DE GESTION DE L'IDENTITÉ DANS LE COMMERCE
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC TS 27008	INFORMATION TECHNOLOGY – SECURITY TECHNIQUES – GUIDELINES FOR THE ASSESSMENT OF INFORMATION SECURITY CONTROLS
NFPA 951	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 100-9	Gouvernance des données-Partie 9 : Intégration sans copie
CAN/CIOSC 103-1:2020	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
CAN/CIOSC 106-1	Découverte des jumeaux numériques pour les environnements bâtis
CAN/CIOSC 106-2	[Disponible uniquement en anglais]
CAN/CIOSC 109-2	Cadre canadien de protection de la confidentialité des informations
IEEE/IEC 61671-2-2016	[Disponible uniquement en anglais]
IEEE 1671.2	[Disponible uniquement en anglais]
IEEE 1671.3	[Disponible uniquement en anglais]
IEEE 1671.4	[Disponible uniquement en anglais]
IEEE 1671.5	[Disponible uniquement en anglais]
IEEE 1671.6	[Disponible uniquement en anglais]
ISO/IEC/IEEE 18881:2016	Technologies de l'information – Protocole de contrôle de la communauté verte omniprésente – Contrôle et gestion
IEEE P802.11bb	[Disponible uniquement en anglais]
CSA Z8003	Recherche et évaluation de la conception des établissements de soins de santé

Question clé 24
intermédiaires du traitement de données de confiance

ETSI TS 133 501	[Disponible uniquement en anglais]
ISO TR 20526	RAPPORT DE L'ÉTAT DE LA TECHNIQUE CONCERNANT LA BILLETTIQUE CENTRÉE SUR LE COMPTE USAGER
ISO TS 8000-150	QUALITÉ DES DONNÉES – PARTIE 150 : DONNÉES PERMANENTES : CADRE DE MANAGEMENT DE LA QUALITÉ

ISO/IEC 15944-12	Technologies de l'information – Vue opérationnelle d'affaires – Partie 12 : Exigences en matière de protection de la vie privée (PPR) relatives à la gestion du cycle de vie de l'information (ILCM) et de l'EDI des renseignements personnels (PI)
ISO/IEC 17788	Technologies de l'information – Informatique en nuage – Vue d'ensemble et vocabulaire
ISO/IEC 17789	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – ARCHITECTURE DE RÉFÉRENCE
ISO/IEC 17826	Technologies de l'information – Interface de management des données du nuage informatique (CDMI)
ISO/IEC 19086-1	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 19086-4	INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 4 : ELÉMENTS DE SÉCURITÉ ET DE PROTECTION DES PII
ISO/IEC 19941	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – INTEROPÉRABILITÉ ET PORTABILITÉ
ISO/IEC 21878	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR LA CONCEPTION ET L'IMPLÉMENTATION SÉCURISÉES DES SERVEURS VIRTUALISÉS
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 24760-3	Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 3 : Mise en œuvre
ISO/IEC 27000	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SYSTÈMES DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION – VUE D'ENSEMBLE ET VOCABULAIRE
ISO/IEC 27009	SÉCURITÉ DE L'INFORMATION, CYBERSÉCURITÉ ET PROTECTION DES DONNÉES PERSONNELLES – APPLICATION DE L'ISO/IEC 27001 À UN SECTEUR SPÉCIFIQUE – EXIGENCES
ISO/IEC 27018	Technologies de l'information – Techniques de sécurité – Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII
ISO/IEC 27036-4	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ D'INFORMATION POUR LA RELATION AVEC LE FOURNISSEUR – PARTIE 4 : LIGNES DIRECTRICES POUR LA SÉCURITÉ DES SERVICES DU NUAGE
ISO/IEC 27701	TECHNIQUES DE SÉCURITÉ – EXTENSION D'ISO/IEC 27001 ET ISO/IEC 27002 AU MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE – EXIGENCES ET LIGNES DIRECTRICES
ISO/IEC 30141	ARCHITECTURE DE RÉFÉRENCE DE L'INTERNET DES OBJETS (IOT RA) – RECTIFICATIF TECHNIQUE 1
ISO/IEC 38505-1	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données
ISO/IEC TR 20000-9	TECHNOLOGIES DE L'INFORMATION – GESTION DES SERVICES – PARTIE 9 : APPLICATION DE L'ISO/IEC 20000-1 AU SERVICES DE CLOUD
ISO/IEC TR 20547-2	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 2 : CAS PRATIQUES ET EXIGENCES DÉRIVÉES
ISO/IEC TR 22678	[Disponible uniquement en anglais]
ISO/IEC TR 23186	[Disponible uniquement en anglais]
ISO/IEC TR 23187	[Disponible uniquement en anglais]
ISO/IEC TR 23188	[Disponible uniquement en anglais]
ISO/IEC TR 27550	Technologies de l'information – Techniques de sécurité – Ingénierie de la vie privée pour les processus du cycle de vie des systèmes
ISO/IEC TR 30164	L'internet des objets (IoT) – Informatique en périphérie
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC TS 20748-4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4 :
ISO/IEC TS 23167	[Disponible uniquement en anglais]

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 103-1	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
Pan-Canadian Trust Framework	Aperçu du cadre de confiance pancanadien : Une approche collaborative pour développer un cadre de confiance pancanadien
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données

Question clé 25
autorisation de collecte et de partage de données

ANSI INCITS 172	[Disponible uniquement en anglais]
ASHRAE 135	[Disponible uniquement en anglais]
ASHRAE 201	[Disponible uniquement en anglais]
ASTM E1578	[Disponible uniquement en anglais]
AWWA G410	[Disponible uniquement en anglais]
BSI BS 10012	[Disponible uniquement en anglais]
BSI BS 10102-1	[Disponible uniquement en anglais]
BSI PAS 1085	[Disponible uniquement en anglais]
BSI PAS 1296	[Disponible uniquement en anglais]
BSI PAS 180	[Disponible uniquement en anglais]
BSI PAS 183	[Disponible uniquement en anglais]
BSI PAS 185	[Disponible uniquement en anglais]
CEN EN 14484	Informatique de santé – Transfert international des données personnelles de santé couvertes par la directive européenne sur la protection des données personnelles – Politique de sécurité de haut niveau
CEN EN 14485	Informatique de santé – Guide pour manipuler des données personnelles de santé dans des applications internationales dans le contexte de la directive européenne sur la protection des données personnelles
CEN/TS 17470	Modèle de service de téléassistance
CSA PLUS 8300-96	[Disponible uniquement en anglais]
CSA PLUS 8830-95	[Disponible uniquement en anglais]
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN SPEC 91357	[Disponible uniquement en anglais]
DS DS/CWA 17145-1	[Disponible uniquement en anglais]
ETSI GS INS 009	[Disponible uniquement en anglais]
ETSI GS MOI 002	[Disponible uniquement en anglais]
ETSI SR 002 564	[Disponible uniquement en anglais]
ETSI SR 003 391	[Disponible uniquement en anglais]

ETSI TR 102 202	[Disponible uniquement en anglais]
ETSI TR 103 304	[Disponible uniquement en anglais]
ETSI TR 103 305	[Disponible uniquement en anglais]
ETSI TR 103 370	[Disponible uniquement en anglais]
ETSI TR 103 591	[Disponible uniquement en anglais]
ETSI TS 103 458	[Disponible uniquement en anglais]
ETSI TS 103 532	[Disponible uniquement en anglais]
ETSI TS 129 240	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
IEEE 26514	[Disponible uniquement en anglais]
IEEE WHITE PAPER 3DBP IC	[Disponible uniquement en anglais]
IEEE WHITE PAPER-0	[Disponible uniquement en anglais]
ISO 13606-4	Informatique de santé – Communication du dossier de santé informatisé – Partie 4 : sécurité
ISO 18308	Informatique de santé – Exigences relatives à une architecture de l'enregistrement électronique en matière de santé
ISO 19115-1	INFORMATION GÉOGRAPHIQUE – MÉTADONNÉES – PARTIE 1 : PRINCIPES DE BASE – AMENDEMENT 2
ISO 19650-5	Organisation et numérisation des informations relatives aux bâtiments et ouvrages de génie civil, y compris modélisation des informations de la construction (BIM) – Gestion de l'information par la modélisation des informations de la construction – Partie 5 : Approche de la gestion de l'information axée sur la sécurité
ISO 20252	ÉTUDES DE MARCHÉ, ÉTUDES SOCIALES ET D'OPINION, Y COMPRIS INSIGHTS ET ANALYTIQUE DE DONNÉES – VOCABULAIRE ET EXIGENCES DE SERVICE
ISO 22857	INFORMATIQUE DE SANTÉ – LIGNES DIRECTRICES SUR LA PROTECTION DES DONNÉES POUR FACILITER LES FLUX D'INFORMATION SUR LA SANTÉ DU PERSONNEL DE PART ET D'AUTRE DES FRONTIÈRES
ISO 24100	Systèmes intelligents de transport – Les principes de base pour la protection des données personnelles de sonde
ISO 24978	Systèmes intelligents de transport – Messages de sûreté et d'urgence pour les SIT utilisant tous les moyens de transmission sans fil disponibles – Procédures d'enregistrement des données
ISO 25237	INFORMATIQUE DE SANTÉ – PSEUDONYMISATION
ISO 26000	LIGNES DIRECTRICES RELATIVES À LA RESPONSABILITÉ SOCIÉTALE
ISO 29134	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – LIGNES DIRECTRICES POUR L'ÉTUDE D'IMPACTS SUR LA VIE PRIVÉE
ISO 35001	Système de management des biorisques en laboratoires et autres organismes associés
ISO 37156	INFRASTRUCTURES URBAINES INTELLIGENTES – CADRE DIRECTEUR POUR L'ÉCHANGE ET LE PARTAGE DE DONNÉES POUR LES INFRASTRUCTURES URBAINES INTELLIGENTES
ISO TR 14639-2	Informatique de santé – Feuille de route de l'architecture de santé électronique fondée sur la capacité – Partie 2 : Composants architecturaux et modèle de maturité
ISO TR 17427-3	SYSTÈMES INTELLIGENTS DE TRANSPORT – SYSTÈMES INTELLIGENTS DE TRANSPORT COOPÉRATIFS – PARTIE 3 : CONCEPT DES OPÉRATIONS (CONOPS) POUR LES SYSTÈMES 'PRINCIPAUX'
ISO TR 17427-7	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 7 : Aspects relatifs à la vie privée
ISO TR 22221	Informatique de santé – Principes et indications d'exploitation d'un entrepôt de données cliniques
ISO TR 22758	Biotechnologie – Biobanking – Guide de mise en œuvre de l'ISO 20387
ISO TS 12812-5	OPÉRATIONS BANCAIRES DE BASE – SERVICES FINANCIERS MOBILES – PARTIE 5 : PAIEMENTS MOBILES À ENTREPRISES

ISO TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO TS 19256	Informatique de santé – Exigences pour les systèmes de dictionnaires de produits médicaux pour les soins de santé
ISO TS 21089	INFORMATIQUE DE SANTÉ – FLUX D'INFORMATIONS "TRUSTED END-TO-END"
ISO TS 21547	INFORMATIQUE DE SANTÉ – EXIGENCES DE SÉCURITÉ POUR L'ARCHIVAGE DES DOSSIERS DE SANTÉ ÉLECTRONIQUES – PRINCIPES
ISO TS 22220	INFORMATIQUE DE SANTÉ – IDENTIFICATION DES SUJETS DE SOINS SANITAIRES
ISO TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ISO TS 37107	Villes et communautés territoriales durables – Modèle de maturité pour des communautés territoriales durables et intelligentes
ISO/IEC 15504-6	TECHNOLOGIES DE L'INFORMATION – ÉVALUATION DES PROCÉDÉS – PARTIE 6 : UN EXEMPLE DE MODÈLE D'ÉVALUATION DES PROCÉDÉS DU CYCLE DE VIE D'UN SYSTÈME
ISO/IEC 15944-9	Technologies de l'information – Vue opérationnelle des affaires – Partie 9 : Cadre de traçabilité des transactions d'affaires pour l'échange d'engagements
ISO/IEC 17789	Technologies de l'information – Informatique en nuage – Architecture de référence
ISO/IEC 18028-1	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE RÉSEAUX TI – PARTIE 1 : GESTION DE SÉCURITÉ DE RÉSEAU
ISO/IEC 18384-2	TECHNOLOGIE DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE POUR L'ARCHITECTURE ORIENTÉE SERVICE (SOA RA) – PARTIE 2 : ARCHITECTURE DE RÉFÉRENCE POUR LES SOLUTIONS DE L'ARCHITECTURE ORIENTÉE SERVICE
ISO/IEC 19790	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – EXIGENCES DE SÉCURITÉ POUR LES MODULES CRYPTOGRAPHIQUES
ISO/IEC 19941	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – INTEROPÉRABILITÉ ET PORTABILITÉ
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO/IEC 20748.1	TECHNOLOGIES POUR L'ÉDUCATION, LA FORMATION ET L'APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 1 : MODÈLE DE RÉFÉRENCE
ISO/IEC 20748.2	TECHNOLOGIES DE L'INFORMATION – ÉDUCATION, FORMATION ET APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 2 : EXIGENCES RELATIVES AU SYSTÈME
ISO/IEC 20748.4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4 :
ISO/IEC 20889	TERMINOLOGIE ET CLASSIFICATION DES TECHNIQUES DE DÉ-IDENTIFICATION DE DONNÉES POUR LA PROTECTION DE LA VIE PRIVÉE
ISO/IEC 20944-1	TECHNOLOGIES DE L'INFORMATION – INTEROPÉRABILITÉ ET LIAISONS DES REGISTRES DE MÉTADONNÉES (MDR-IB) – PARTIE 1 : CADRE D'APPLICATIONS, VOCABULAIRE COMMUN ET DISPOSITIONS COMMUNES DE CONFORMITÉ
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 23092-1	Technologie de l'information – Représentation des informations génomiques – Partie 1 : Transport et stockage des informations génomiques
ISO/IEC 23092-2	Technologies de l'information – Représentation des informations génomiques – Partie 2 : Codage des informations génomiques
ISO/IEC 23092-3	TECHNOLOGIE DE L'INFORMATION – REPRÉSENTATION DES INFORMATIONS GÉNOMIQUES – PARTIE 3 : MÉTADONNÉES ET INTERFACES DE PROGRAMMATION D'APPLICATION (API)
ISO/IEC 24760-1	Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 1 : Terminologie et concepts

ISO/IEC 24760-2	Technologies de l'information – Techniques de sécurité – Cadre pour le gestion de l'identité – Partie 2 : Architecture de référence et exigences
ISO/IEC 24760-3	Technologies de l'information – Techniques de sécurité – Cadre pour la gestion de l'identité – Partie 3 : Mise en œuvre
ISO/IEC 27033-1	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE RÉSEAU – PARTIE 1 : VUE D'ENSEMBLE ET CONCEPTS
ISO/IEC 27701	TECHNIQUES DE SÉCURITÉ – EXTENSION D'ISO/IEC 27001 ET ISO/IEC 27002 AU MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE – EXIGENCES ET LIGNES DIRECTRICES
ISO/IEC 29155-4	Ingénierie des systèmes et du logiciel – Cadre de conduite de tests de performance de projet de technologies de l'information – Partie 4 : Directives pour la collecte de données et la maintenance
ISO/IEC 30141	Architecture de référence de l'Internet des objets (IoT RA)
ISO/IEC/IEEE 12207	SYSTEMS AND SOFTWARE ENGINEERING – SOFTWARE LIFE CYCLE PROCESSES
ISO/IEC/IEEE 15288	Ingénierie des systèmes et du logiciel – Processus du cycle de vie du système
ISO/IEC/IEEE 23026	Ingénierie des systèmes et du logiciel – Ingénierie et gestion de sites web pour les systèmes, logiciels et services d'information
ISO/IEC/IEEE 24748-1	Ingénierie des systèmes et du logiciel – Gestion du cycle de vie – Partie 1 : Lignes directrices pour la gestion du cycle de vie
ISO/IEC/IEEE 29148	Ingénierie des systèmes et du logiciel – Processus du cycle de vie – Ingénierie des exigences
ISO/IEC/TR 13335-4	TECHNOLOGIES DE L'INFORMATION – LIGNES DIRECTRICES POUR LA GESTION DE SÉCURITÉ IT – PARTIE 4 : SÉLECTION DE SAUVEGARDES
ISO/IEC/TR 20748-1	TECHNOLOGIES POUR L'ÉDUCATION, LA FORMATION ET L'APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 1 : MODÈLE DE RÉFÉRENCE
ISO/IEC/TR 20748-2	TECHNOLOGIES DE L'INFORMATION – ÉDUCATION, FORMATION ET APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 2 : EXIGENCES RELATIVES AU SYSTÈME
ISO/IEC/TR 23186	[Disponible uniquement en anglais]
ISO/IEC/TR 23188	[Disponible uniquement en anglais]
ISO/IEC/TR 24714-1	Technologies de l'information – Biométrie – Considérations juridictionnelles et sociétales pour applications commerciales – Partie 1 : Guidage général
ISO/IEC/TR 27550	Technologies de l'information – Techniques de sécurité – Ingénierie de la vie privée pour les processus du cycle de vie des systèmes
ISO/IEC/TR 29144	TECHNOLOGIES DE L'INFORMATION – BIOMÉTRIQUE – UTILISATION DE LA TECHNOLOGIE BIOMÉTRIQUE DANS LES PROCESSUS ET LES APPLICATIONS DE GESTION DE L'IDENTITÉ DANS LE COMMERCE
ISO/IEC/TR 29196	Technologies de l'information – Directives pour l'inscription biométrique
ISO/TR 14639-2	Informatique de santé – Feuille de route de l'architecture de santé électronique fondée sur la capacité – Partie 2 : Composants architecturaux et modèle de maturité
ISO/TR 17424	Systèmes intelligents de transport – Systèmes coopératifs – État des connaissances des cartes dynamiques locales
ISO/TR 17427-3	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 3 : Concept des opérations (ConOps) pour les systèmes 'principaux'
ISO/TR 17427-7	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 7 : Aspects relatifs à la vie privée
ISO/TR 17427-9	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 9 : Conformité et aspects relatifs à l'application
ISO/TR 17465-2	Systèmes intelligents de transport – Coopérative ITS – Partie 2 : Lignes directrices pour les documents normatifs
ISO/TR 18638	Informatique de santé – Composantes éducatives destinées à garantir la confidentialité des informations relatives à la santé

ISO/TR 21548	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Lignes directrices
ISO/TR 22221	Informatique de santé – Principes et indications d'exploitation d'un entrepôt de données cliniques
ISO/TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO/TS 19256	Informatique de santé – Exigences pour les systèmes de dictionnaires de produits médicaux pour les soins de santé
ISO/TS 21089	INFORMATIQUE DE SANTÉ – FLUX D'INFORMATIONS "TRUSTED END-TO-END"
ISO/TS 21547	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Principes
ISO/TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ISO/TS 37107	Villes et communautés territoriales durables – Modèle de maturité pour des communautés territoriales durables et intelligentes
ITU-T M.3363	Exigences pour la gestion des données dans le réseau de gestion des télécommunications
ITU-T SERIES X SUPP 32	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 49	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 56	[Disponible uniquement en anglais]
ITU-T X.1045	Architecture de la chaîne de services de sécurité pour les réseaux et les applications
ITU-T X.1209	Capacités et scénarios de contexte associés pour le partage et l'échange d'informations sur la cybersécurité
ITU-T X.1361	[Disponible uniquement en anglais]
ITU-T X.1363	[Disponible uniquement en anglais]
ITU-T Y.2705	Exigences minimales de sécurité de l'interconnexion pour le service de télécommunications d'urgence (ETS)
ITU-T Y.3518	Informatique en nuage – Exigences fonctionnelles de la gestion de données inter-nuages
ITU-T Y.3519	Informatique en nuage – Architecture fonctionnelle des mégadonnées en tant que service
ITU-T Y.3600	Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage
ITU-T Y.4117	Exigences et capacités de l'Internet des objets pour la prise en charge des dispositifs à porter sur soi et des services connexes
ITU-T Y.4500.2	[Disponible uniquement en anglais]
ITU-T Y.4555	Fonctionnalités de service d'auto-quantification dans l'Internet des objets
ITU-T Y.4904	Modèle de maturité pour les villes intelligentes et durables
SAE AIR6904	[Disponible uniquement en anglais]
SAE EIA-836B	[Disponible uniquement en anglais]
SNZ HB 246	[Disponible uniquement en anglais]
UL 2800 BULLETIN	[Disponible uniquement en anglais]
ULC CAN/ULC-S576	NORME SUR L'ÉQUIPEMENT ET LES ACCESSOIRES DES SYSTÈMES DE NOTIFICATION DE MASSE
ISO TR 14872	INFORMATIQUE DE SANTÉ – IDENTIFICATION DES MÉDICAMENTS – PRINCIPES ESSENTIELS POUR LA MISE À JOUR DES IDENTIFIANTS ET DES TERMES
ISO 18750	Système de transports intelligents – Systèmes coopératifs – Carte locale dynamique
ISO/IEC TR 20748-1	TECHNOLOGIES POUR L'ÉDUCATION, LA FORMATION ET L'APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 1 : MODÈLE DE RÉFÉRENCE
ETSI TS 102 573	[Disponible uniquement en anglais]

AWWA G430	[Disponible uniquement en anglais]
ISO/IEC 22624	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
IEEE P3333.2.3	[Disponible uniquement en anglais]

Question clé 26 chiffrement

ANSI INCITS 504-1	[Disponible uniquement en anglais]
ANSI INCITS 504-3	[Disponible uniquement en anglais]
ANSI X9 TR-48	[Disponible uniquement en anglais]
ANSI X9.69	[Disponible uniquement en anglais]
ANSI X9.73	[Disponible uniquement en anglais]
ASHRAE 135	[Disponible uniquement en anglais]
ASHRAE HVAC APPLICATIONS SI CH 40	[Disponible uniquement en anglais]
BSI BS 10008-2	[Disponible uniquement en anglais]
BSI DD ENV 13608-1	[Disponible uniquement en anglais]
BSI BS 10012 + A1	[Disponible uniquement en anglais]
BSI PD CEN/TR 16742	[Disponible uniquement en anglais]
CEN 15320	Systèmes de cartes d'identification – Applications pour le transport terrestre – Applications de transport public interopérables
CEN 15531-2	Transport public – Interface de service pour les informations en temps réel relatives aux opérations de transport public – Partie 2 : Infrastructure des communications
CEN 16312	Systèmes de transport intelligents – Identification automatique des véhicules et des équipements (AVI/AEI) – Profil d'application d'interopérabilité pour AVI/AEI et identification d'enregistrement électronique en utilisant des systèmes de communication dédiés à courte portée
CSA PLUS 8300-96	[Disponible uniquement en anglais]
CSA PLUS 8830-95	[Disponible uniquement en anglais]
DIN 66398	[Disponible uniquement en anglais]
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN CEN/TS 16634	Identification personnelle – Recommandations pour l'usage de la biométrie lors des contrôles automatisés aux frontières de l'Europe
ETSI GR NFV 001	[Disponible uniquement en anglais]

ETSI GR NFV-SEC 003	[Disponible uniquement en anglais]
ETSI GR NFV-SEC 009	[Disponible uniquement en anglais]
ETSI GR QSC 001	[Disponible uniquement en anglais]
ETSI GR QSC 003	[Disponible uniquement en anglais]
ETSI GR QSC 004	[Disponible uniquement en anglais]
ETSI GR QSC 006	[Disponible uniquement en anglais]
ETSI GS ENI 005	[Disponible uniquement en anglais]
ETSI GS INS 005	[Disponible uniquement en anglais]
ETSI GS NFV-SEC 001	[Disponible uniquement en anglais]
ETSI GS NFV-SEC 006	[Disponible uniquement en anglais]
ETSI GS NFV-SEC 013	[Disponible uniquement en anglais]
ETSI GS NGP 001	[Disponible uniquement en anglais]
ETSI SR 003 391	[Disponible uniquement en anglais]
ETSI TR 102 935	[Disponible uniquement en anglais]
ETSI TR 103 304	[Disponible uniquement en anglais]
ETSI TR 103 305	[Disponible uniquement en anglais]
ETSI TR 103 305-1	[Disponible uniquement en anglais]
ETSI TR 103 305-3	[Disponible uniquement en anglais]
ETSI TR 103 308	[Disponible uniquement en anglais]
ETSI TR 103 376	[Disponible uniquement en anglais]
ETSI TR 103 456	[Disponible uniquement en anglais]
ETSI TR 103 509	[Disponible uniquement en anglais]
ETSI TR 103 533	[Disponible uniquement en anglais]
ETSI TR 103 591	[Disponible uniquement en anglais]
ETSI TS 102 412	[Disponible uniquement en anglais]
ETSI TS 103 458	[Disponible uniquement en anglais]
ETSI TS 118 103	[Disponible uniquement en anglais]
ETSI TR 103 370	[Disponible uniquement en anglais]
ETSI GS MOI 002	[Disponible uniquement en anglais]
ETSI TR 102 935	[Disponible uniquement en anglais]
ETSI TS 118 103	[Disponible uniquement en anglais]
ETSI TR 103 582	Étude de cas et de communications d'utilisation impliquant des dispositifs d'IoT dans équipement de situations d'urgence
ETSI TS 103 485	[Disponible uniquement en anglais]
ETSI TR 102 937	[Disponible uniquement en anglais]
IEC 62443-2-4	Sécurité des automatismes industriels et des systèmes de commande – Partie 2-4 : Exigences de programme de sécurité pour les fournisseurs de service IACS
IEC 62443-3-3	Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes – Partie 3-3 : Exigences de sécurité des systèmes et niveaux de sécurité
IEC 62443-4-2	Sécurité des systèmes d'automatisation et de commande industrielles – Partie 4-2 : Exigences de sécurité technique des composants IACS
IEC/TR 62939-1	[Disponible uniquement en anglais]
IEC/TS 62045-1	[Disponible uniquement en anglais]

IEEE 1619	[Disponible uniquement en anglais]
IEEE 1619.2	[Disponible uniquement en anglais]
IEEE 1703	[Disponible uniquement en anglais]
IEEE 23026	Ingénierie des systèmes et du logiciel – Ingénierie et gestion de sites web pour les systèmes, logiciels et services d'information
IEEE 2410	[Disponible uniquement en anglais]
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	[Disponible uniquement en anglais]
IEEE 2600	[Disponible uniquement en anglais]
ISO 11073-90101	INFORMATIQUE DE SANTÉ – COMMUNICATION ENTRE DISPOSITIFS MÉDICAUX SUR LE SITE DES SOINS – PARTIE 90101 : INSTRUMENTS ANALYTIQUES – ESSAI SUR LE SITE DES SOINS
ISO 16484-3	SYSTÈMES DE GESTION TECHNIQUE DU BÂTIMENT (SGTB) – PARTIE 3 : FONCTIONS
ISO 16484-5	SYSTÈMES D'AUTOMATISATION ET DE GESTION TECHNIQUE DU BÂTIMENT – PARTIE 5 : PROTOCOLE DE COMMUNICATION DE DONNÉES
ISO 20214	SYSTÈMES DE TRANSFERT DES INFORMATIONS ET DONNÉES SPATIALES – ARCHITECTURE DE SÉCURITÉ POUR LES SYSTÈMES DE DONNÉES SPATIALES
ISO TR 11636	INFORMATIQUE DE SANTÉ – RÉSEAU PRIVÉ, VIRTUEL, DYNAMIQUE, SUR DEMANDE POUR INFRASTRUCTURE D'INFORMATION DE SANTÉ
ISO TR 17427-3	SYSTÈMES INTELLIGENTS DE TRANSPORT – SYSTÈMES INTELLIGENTS DE TRANSPORT COOPÉRATIFS – PARTIE 3 : CONCEPT DES OPÉRATIONS (CONOPS) POUR LES SYSTÈMES 'PRINCIPAUX'
ISO TR 23244	[Disponible uniquement en anglais]
ISO TR 23455	[Disponible uniquement en anglais]
ISO TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO TS 21089	Informatique de santé – Flux d'informations "trusted end-to-end"
ISO TS 22220	INFORMATIQUE DE SANTÉ – IDENTIFICATION DES SUJETS DE SOINS SANITAIRES
ISO TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ISO/IEC 15408-2	Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI – Partie 2 : Composants fonctionnels de sécurité
ISO/IEC 17789	Technologies de l'information – Informatique en nuage – Architecture de référence
ISO/IEC 18033-6	Techniques de sécurité IT – Algorithmes de chiffrement – Partie 6 : Chiffrement homomorphe
ISO/IEC 20889	TERMINOLOGIE ET CLASSIFICATION DES TECHNIQUES DE DÉ-IDENTIFICATION DE DONNÉES POUR LA PROTECTION DE LA VIE PRIVÉE
ISO/IEC 25023	Ingénierie des systèmes et du logiciel – Exigences de qualité et évaluation des systèmes et du logiciel (SQuaRE) – Mesurage de la qualité du produit logiciel et du système
ISO/IEC 27017	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CODE DE BONNES PRATIQUES POUR LES CONTRÔLES DE SÉCURITÉ DE L'INFORMATION FONDÉS SUR L'ISO/IEC 27002 POUR LES SERVICES DU NUAGE
ISO/IEC 27033-1	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE RÉSEAU – PARTIE 1 : VUE D'ENSEMBLE ET CONCEPTS
ISO/IEC 27033-3	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE RÉSEAU – PARTIE 3 : SCÉNARIOS DE RÉSEAUTAGE DE RÉFÉRENCE – MENACES, TECHNIQUES CONCEPTUELLES ET QUESTIONS DE CONTRÔLE
ISO/IEC 27040	TECHNOLOGIE DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DE STOCKAGE
ISO/IEC 27050-1	TECHNOLOGIES DE L'INFORMATION – DÉCOUVERTE ÉLECTRONIQUE – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS

ISO/IEC 29101	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – ARCHITECTURE DE RÉFÉRENCE DE LA PROTECTION DE LA VIE PRIVÉE
ISO/IEC 29151	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – CODE DE BONNE PRATIQUE POUR LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL
ISO/IEC 30118-2	TECHNOLOGIES DE L'INFORMATION – SPÉCIFICATION DE LA FONDATION POUR LA CONNECTIVITÉ OUVERTE (FONDATION OCF) – PARTIE 2 : SPÉCIFICATION DE SÉCURITÉ
ISO/IEC 30136	Technologies de l'information – Essais de performance des systèmes de protection par modèle
ISO/IEC 38505.2	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – PARTIE 2 : IMPLICATIONS DE L'ISO/IEC 38505-1 POUR LA GESTION DES DONNÉES
ISO/IEC TR 22678	[Disponible uniquement en anglais]
ISO/IEC TR 23188	[Disponible uniquement en anglais]
ISO/IEC TR 24028	TECHNOLOGIES DE L'INFORMATION – INTELLIGENCE ARTIFICIELLE – EXAMEN D'ENSEMBLE DE LA FIABILITÉ EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE
ISO/IEC TR 24714-1	Technologies de l'information – Biométrie – Considérations juridictionnelles et sociétales pour applications commerciales – Partie 1 : Guidage général
ISO/IEC TR 27550	Technologies de l'information – Techniques de sécurité – Ingénierie de la vie privée pour les processus du cycle de vie des systèmes
ISO/IEC TR 29181-2	Technologies de l'information – Réseaux du futur – Énoncé du problème et exigences – Partie 2 : Dénomination et adressage
ISO/IEC TR 30164	L'INTERNET DES OBJETS (IOT) – INFORMATIQUE EN PÉRIPHÉRIE
ISO/IEC TR 30166	L'internet des objets (IoT) – L'internet industriel des objets
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/IEC TS 20540	Technologies de l'information – Techniques de sécurité – Test de modules cryptographiques dans leur environnement d'exploitation
ISO/IEC TS 23167	[Disponible uniquement en anglais]
ISO/IEC/IEEE 23026	Ingénierie des systèmes et du logiciel – Ingénierie et gestion de sites web pour les systèmes, logiciels et services d'information
ISO/TR 11636	Informatique de santé – Réseau privé, virtuel, dynamique, sur demande pour infrastructure d'information de santé
ISO/TR 17427-3	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 3 : Concept des opérations (ConOps) pour les systèmes 'principaux'
ISO/TR 18307	Informatique de santé – interopérabilité et compatibilité avec les normes de messagerie et de communication – caractéristiques
ISO/TR 21548	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Lignes directrices
ISO/TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO/TS 21089	INFORMATIQUE DE SANTÉ – FLUX D'INFORMATIONS "TRUSTED END-TO-END"
ISO/TS 21547	Informatique de santé – Exigences de sécurité pour l'archivage des dossiers de santé électroniques – Principes
ISO/TS 22220	Informatique de santé – Identification des sujets de soins sanitaires
ISO/TS 27790	Informatique de santé – Cadre d'enregistrement de document
ISO/TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ISO 25237	INFORMATIQUE DE SANTÉ – PSEUDONYMISATION
ISO/IEC TS 27008 – TC	Technologies de l'information – Techniques de sécurité – Lignes directrices pour les auditeurs des contrôles de sécurité de l'information

ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO/TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ISO/TS 14265	Informatique de santé – Classification des besoins pour le traitement des informations de santé personnelles
ISO/TR 22221	Informatique de santé – Principes et indications d'exploitation d'un entrepôt de données cliniques
ISO/TS 17975	Informatique de santé – Principes et exigences des données pour le consentement dans la collecte, l'utilisation ou la divulgation d'informations de santé personnelles
ISO 22857	INFORMATIQUE DE SANTÉ – LIGNES DIRECTRICES SUR LA PROTECTION DES DONNÉES POUR FACILITER LES FLUX D'INFORMATION SUR LA SANTÉ DU PERSONNEL DE PART ET D'AUTRE DES FRONTIÈRES
ISO/IEC TS 20748-4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4 :
ISO/IEC TS 20748-4:20	Technologies pour l'éducation, la formation et l'apprentissage – Interopérabilité de l'analytique de l'apprentissage – Partie 4 : N/A
ISO/IEC 27011	Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour les contrôles de la sécurité de l'information fondés sur l'ISO/IEC 27002 pour les organismes de télécommunications
ISO/IEC 29100	Technologies de l'information – Techniques de sécurité – Cadre privé
ISO/TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO 5127	INFORMATION ET DOCUMENTATION – FONDATIONS ET VOCABULAIRE
ISO 27799	INFORMATIQUE DE SANTÉ – MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION RELATIVE À LA SANTÉ EN UTILISANT L'ISO/IEC 27002
ISO/TR 17427-7	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 7 : Aspects relatifs à la vie privée
ISO/IEC 19506	Technologies de l'information – Modernisation conduite par l'architecture (ADM) de l'OMG – Métamodèle de découverte de connaissances (KDM)
ISO/IEC 27034-1	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – SÉCURITÉ DES APPLICATIONS – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 29151	Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour la protection des données à caractère personnel
ITU-T H.810	Directives de conception visant à assurer l'interopérabilité des systèmes de santé connectée individuels : Introduction
ITU-T J.191	Paquetage de fonctionnalités IP pour l'amélioration des câblo-modems
ITU-T SERIES Y SUPP 49	[Disponible uniquement en anglais]
ITU-T X.1039	Mesures de sécurité techniques pour la mise en oeuvre des dimensions de sécurité UIT-T X.805
ITU-T X.1045	Architecture de la chaîne de services de sécurité pour les réseaux et les applications
ITU-T X.1361	[Disponible uniquement en anglais]
ITU-T X.1401	Menaces de sécurité pour la technologie des registres distribués
ITU-T X.1602	[Disponible uniquement en anglais]
ITU-T X.1642	[Disponible uniquement en anglais]
ITU-T X.894	[Disponible uniquement en anglais]
ITU-T Y.2342	Scénarios et exigences relatives aux capacités pour la chaîne de blocs pour l'évolution des réseaux de prochaine génération
ITU-T Y.3502	Technologies de l'information – Informatique en nuage – Architecture de référence
ITU-T Y.3505	Informatique en nuage – Aperçu et exigences fonctionnelles pour la fédération du stockage des données

ITU-T Y.3509	Informatique en nuage – Architecture fonctionnelle pour la fédération du stockage des données
ITU-T Y.3518	Informatique en nuage – Exigences fonctionnelles de la gestion de données inter-nuages
ITU-T Y.3524	Exigences et cadre de maturité pour l'informatique en nuage
ITU-T Y.3800	Aperçu des réseaux prenant en charge la distribution de clés quantiques
ITU-T Y.4459	Cadre de l'architecture d'entité numérique pour l'interopérabilité dans l'Internet des objets
ITU-T Y.3501	Informatique en nuage – Cadre et exigences de haut niveau
ITU-T H.780	Affichage numérique : Spécifications du service et architecture fondée sur la TVIP
NEMA C12.22	[Disponible uniquement en anglais]
UL CAN/UL 2900-1	Cybersécurité des logiciels pour les produits à connexion réseau, partie 1 : exigences générales
UL SUBJECT 2900-1	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 103-1:2020	Confiance et identité numérique – Partie 1 : Notions fondamentales
CAN/CIOSC 103-2	Confiance et identité numérique – Partie 2 : Prestation de services de santé
IEEE Std 2410-2019	[Disponible uniquement en anglais]
IEEE Std 1363.3-2013	[Disponible uniquement en anglais]
IEEE 1619.1-2018	[Disponible uniquement en anglais]
IEEE 1735-2014	[Disponible uniquement en anglais]
IEEE P802.15.4y	[Disponible uniquement en anglais]
IEEE 802.1AEcg-2017	[Disponible uniquement en anglais]
IEEE/ISO/IEC 8802-1AE:2013/Amd.3-2018 -	[Disponible uniquement en anglais]
IEEE 1609.2b-2019	[Disponible uniquement en anglais]
IEEE 8802-1AE:2013/ Amd.1-2015	[Disponible uniquement en anglais]
IEEE ST 429-6:2006 Am1:2018	[Disponible uniquement en anglais]

Question clé 27
gestion des ontologies

ITU-T Y.2076	Exigences et cadre sémantiques de l'Internet des objets
ITU-T Y.3600	Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage
ITU-T Y.3601	Mégadonnées – Cadre et exigences pour l'échange de données
ITU-T Y.4203	Exigences relatives à la description des objets dans l'Internet des objets
ITU-T Y.4461	Cadre de données ouvertes dans les villes intelligentes

ISO/TS 13606-4	Informatique de santé – Communication du dossier de santé informatisé – Partie 4 : sécurité
ETSI TR 103 537	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
ETSI GS MOI 010	[Disponible uniquement en anglais]
ANSI INCITS 532	[Disponible uniquement en anglais]
DIN SPEC 91349	[Disponible uniquement en anglais]
DIN SPEC 91357	[Disponible uniquement en anglais]
ETSI SR 003 680	[Disponible uniquement en anglais]
ETSI TR 103 411	[Disponible uniquement en anglais]
ETSI TR 103 509	[Disponible uniquement en anglais]
ISO 13606-1	Informatique de santé – Communication du dossier de santé informatisé – Partie 1 : Modèle de référence
ISO 8000-115	QUALITÉ DES DONNÉES – PARTIE 115 : DONNÉES PERMANENTES : ÉCHANGE DES IDENTIFICATEURS QUALITÉ : EXIGENCES SYNTAXIQUES, SÉMANTIQUES ET DE RÉSOLUTION
ISO 8000-116	QUALITÉ DES DONNÉES – PARTIE 116 : DONNÉES PERMANENTES : ÉCHANGE DES IDENTIFICATEURS QUALITÉ : APPLICATION DE L'ISO 8000-115 À LA MISE EN FORME DES IDENTIFICATEURS OFFICIELS D'ENTITÉS JURIDIQUES
ISO 8000-120	Qualité des données – Partie 120 : Données permanentes : Échange des données caractéristiques : Provenance
ISO 8000-130	QUALITÉ DES DONNÉES – PARTIE 130 : DONNÉES PERMANENTES : ÉCHANGE DE DONNÉES CARACTÉRISTIQUES : EXACTITUDE
ISO 8000-140	QUALITÉ DES DONNÉES – PARTIE 140 : DONNÉES PERMANENTES : ÉCHANGE DE DONNÉES CARACTÉRISTIQUES : COMPLÉTUDE
ISO 8000-2	QUALITÉ DES DONNÉES – PARTIE 2 : VOCABULAIRE
ISO/IEC 11179-1	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 1 : CADRE DE RÉFÉRENCE
ISO/IEC 11179-3	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 3 : MÉTAMODÈLE DE REGISTRE ET ATTRIBUTS DE BASE – AMENDEMENT 1
ISO/IEC 11179-5	Technologies de l'information – Registres de métadonnées (RM) – Partie 5 : Principes de dénomination
ISO/IEC 11179-6	Technologies de l'information – Registres de métadonnées (RM) – Partie 6 : Enregistrement des données
ISO/IEC 11179-7	Technologies de l'information – Registres de métadonnées (RM) – Partie 7 : N/A
ISO/IEC 15026.1	Ingénierie des systèmes et du logiciel – Assurance des systèmes et du logiciel – Partie 1 : Concepts et vocabulaire
ISO/IEC 16680	TECHNOLOGIES DE L'INFORMATION – MODÈLE DE MATURITÉ D'INTÉGRATION DU SERVICE DE GROUPE OUVERT (OSIMM)
ISO/IEC 19763-1	Technologies de l'information – Cadre du métamodèle pour l'interopérabilité (MFI) – Partie 1 : Structure
ISO/IEC 19763-3	Technologies de l'information – Cadre du métamodèle pour l'interopérabilité (MFI) – Partie 3 : Métamodèle pour l'enregistrement de l'ontologie
ISO/IEC 19763-5	Technologies de l'information – Cadre du métamodèle pour l'interopérabilité (MFI) – Partie 5 : Métamodèle pour l'enregistrement du modèle de procédé
ISO/IEC 19763-6	TECHNOLOGIES DE L'INFORMATION – CADRE DU MÉTAMODÈLE POUR L'INTEROPÉRABILITÉ (MFI) – PARTIE 6 : RÉSUMÉ REGISTRY
ISO/IEC 19763-7	Technologies de l'information – Cadre du métamodèle pour l'interopérabilité (MFI) – Partie 7 : Métamodèle pour l'enregistrement du modèle de service
ISO/IEC 20547-3	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES MÉGADONNÉES – PARTIE 3 : ARCHITECTURE DE RÉFÉRENCE
ISO/IEC 24707	Technologies de l'information – Logique Commune (CL) – Cadre pour une famille des langages logique-basés

ISO/IEC 30182	MODÈLE DE CONCEPT DE VILLE INTELLIGENTE – LIGNES DIRECTRICES POUR ÉTABLIR UN MODÈLE D'INTEROPÉRABILITÉ DES DONNÉES
ISO/IEC TR 19583-1	Technologies de l'information – Concepts et utilisation des métadonnées – Partie 1 : Concepts liés aux métadonnées
ISO/IEC TR 20547-5	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 5 : FEUILLE DE ROUTE POUR LES NORMES
ISO/IEC TR 20943-1	TECHNOLOGIES DE L'INFORMATION – PROCÉDURES EN VUE D'OBTENIR LA COHÉRENCE DU CONTENU D'UN REGISTRE DE METADONNÉES – PARTIE 1 : ÉLÉMENTS DE DONNÉES
ISO/IEC TR 20943-5	TECHNOLOGIES DE L'INFORMATION —PROCÉDURES POUR RÉALISER LA CONSISTANCE DU CONTENU DE L'ENREGISTREMENT DES MÉTADONNÉES – PARTIE 5 : PROCÉDURE DE MAPPAGE DES MÉTADONNÉES
ISO/IEC TR 20943-6	TECHNOLOGIES DE L'INFORMATION —PROCÉDURES POUR RÉALISER LA CONSISTANCE DU CONTENU DE L'ENREGISTREMENT DES MÉTADONNÉES – PARTIE 6 : CADRE POUR GÉNÉRER DES ONTOLOGIES
ISO/IEC TS 19763-13	Technologies de l'information – Cadre du métamodèle pour l'interopérabilité (MFI) – Partie 13 : Métamodèle pour l'enregistrement de la conception des formulaires
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
IEEE Std 2755-2017	[Disponible uniquement en anglais]
IEEE Std 1636.1-2018	[Disponible uniquement en anglais]
IEEE 11073-10101-2019	[Disponible uniquement en anglais]
ISO/IEC/IEEE 24765:2017	Ingénierie des systèmes et du logiciel – Vocabulaire

Question clé 28
traitement, transparence et traçabilité des données

ANSI INCITS 442	[Disponible uniquement en anglais]
ASTM C1009 REV A	[Disponible uniquement en anglais]
ASTM E1714	[Disponible uniquement en anglais]
ASTM E1931	[Disponible uniquement en anglais]
BSI BS 8593	[Disponible uniquement en anglais]
BSI PAS 180	[Disponible uniquement en anglais]
BSI PAS 212	[Disponible uniquement en anglais]
CGSB CAN/CGSB-72.34	Enregistrements électroniques utilisés à titre de preuves documentaires
CSA PLUS 8300-96	[Disponible uniquement en anglais]
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN SPEC 91357	[Disponible uniquement en anglais]
ETSI GR PDL 001	[Disponible uniquement en anglais]
ETSI GS CIM 006	[Disponible uniquement en anglais]
ETSI GS CIM 009	[Disponible uniquement en anglais]
ETSI GS INS 005	[Disponible uniquement en anglais]
ETSI GS INS 008	[Disponible uniquement en anglais]

ETSI TR 103 535	[Disponible uniquement en anglais]
ETSI TR 103 536	[Disponible uniquement en anglais]
ETSI TR 103 603	[Disponible uniquement en anglais]
ETSI TS 101 533-1	[Disponible uniquement en anglais]
ISO 16175-2	INFORMATION ET DOCUMENTATION – PRINCIPES ET EXIGENCES FONCTIONNELLES POUR LES ENREGISTREMENTS DANS LES ENVIRONNEMENTS ÉLECTRONIQUES DE BUREAU – PARTIE 2 : LIGNES DIRECTRICES ET EXIGENCES FONCTIONNELLES POUR LES SYSTÈMES DE MANAGEMENT DES ENREGISTREMENTS NUMÉRIQUES
ISO 21965	INFORMATION ET DOCUMENTATION – GESTION DES DOCUMENTS D'ACTIVITÉ DANS LES ARCHITECTURES (DES SYSTÉMES D'INFORMATION) D'ENTREPRISE
ISO 25237	Informatique de santé – Pseudonymisation
ISO 30401	Systèmes de management des connaissances – Exigences
ISO 5841-2	Implants chirurgicaux – Stimulateurs cardiaques – Partie 2 : Établissement d'un rapport concernant le fonctionnement clinique de populations de générateurs d'impulsions ou de fils-électrodes
ISO TR 14639-2	Informatique de santé – Feuille de route de l'architecture de santé életronique fondée sur la capacité – Partie 2 : Composants architecturaux et modèle de maturité
ISO TR 19669	Informatique de santé – Stratégie de composants réutilisables pour le développement de cas pratiques
ISO TR 21965	Information et documentation – Gestion des documents d'activité dans les architectures (des systèmes d'information) d'entreprise
ISO TR 22221	Informatique de santé – Principes et indications d'exploitation d'un entrepôt de données cliniques
ISO TS 19256	Informatique de santé – Exigences pour les systèmes de dictionnaires de produits médicaux pour les soins de santé
ISO/IEC 19763-1	Technologies de l'information – Cadre du métamodèle pour l'interopérabilité (MFI) – Partie 1 : Structure
ISO/IEC 30108-1	Technologies de l'information – Service d'assurance de l'identité biométrique (BIAS) – Partie 1 : Services BIAS
ISO/IEC 30182	MODÈLE DE CONCEPT DE VILLE INTELLIGENTE – LIGNES DIRECTRICES POUR ÉTABLIR UN MODÈLE D'INTEROPÉRABILITÉ DES DONNÉES
ISO/IEC 38505.2	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – PARTIE 2 : IMPLICATIONS DE L'ISO/IEC 38505-1 POUR LA GESTION DES DONNÉES
ISO/IEC 38505-1	Technologies de l'information – Gouvernance des technologies de l'information – Gouvernance des données – Partie 1 : Application de l'ISO/IEC 38500 à la gouvernance des données
ISO/IEC TR 16501	Technologies de l'information – Systèmes audiovisuels numériques génériques – Rapport technique sur l'ISO/CEI 16500 – Description des fonctionnalités audiovisuelles numériques
ISO/IEC TR 20547-2	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 2 : CAS PRATIQUES ET EXIGENCES DÉRIVÉES
ISO/IEC TR 23186	[Disponible uniquement en anglais]
ISO/IEC TR 24028	TECHNOLOGIES DE L'INFORMATION – INTELLIGENCE ARTIFICIELLE – EXAMEN D'ENSEMBLE DE LA FIABILITÉ EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données
ISO/TR 14639-2	Informatiques de santé – Feuille de route de l'architecture de santé eletronique fondée sur la capacité – Partie 2 : Composants architecturaux et modèle de maturité
ISO/TR 19669	Informatique de santé – Stratégie de composants réutilisables pour le développement de cas pratiques
ISO/TR 22221	Informatique de santé – Principes et indications d'exploitation d'un entrepôt de données cliniques
ISO/TS 19256	Informatique de santé – Exigences pour les systèmes de dictionnaires de produits médicaux pour les soins de santé

ISO/TS 29585	Informatique de santé – Déploiement d'un entrepôt des données cliniques
ITU-T X.1602	[Disponible uniquement en anglais]
ITU-T Y.3505	Informatique en nuage – Aperçu et exigences fonctionnelles pour la fédération du stockage des données
ITU-T Y.3509	Informatique en nuage – Architecture fonctionnelle pour la fédération du stockage des données
ITU-T Y.3602	Mégadonnées – Exigences fonctionnelles relatives à la provenance des données
ITU-T Y.4464	Cadre de la chaîne de blocs d'objets en tant que plate-forme de services décentralisée
SAE PT-186/11	[Disponible uniquement en anglais]
SNZ AS/NZS 5667.1	[Disponible uniquement en anglais]
SNZ NZS 5259	[Disponible uniquement en anglais]
SNZ SA/SNZ HB 168	[Disponible uniquement en anglais]
UL 2800 BULLETIN	[Disponible uniquement en anglais]
BSI BS 7958 – TC	[Disponible uniquement en anglais]
CEN EN 9300-002	Série aérospatiale – LOTAR – Archivage Long Terme et récupération des données techniques produits numériques, telles que 3D, CAO et PDM – Partie 002 : Exigences
ISO 13606-1 – TC	Informatique de santé – Communication du dossier de santé informatisé – Partie 1 : Modèle de référence
ISO 21090	Informatique de santé – Types de données harmonisées pour une interchangeabilité d'informations
ISO 13606-1	Informatique de santé – Communication du dossier de santé informatisé – Partie 1 : Modèle de référence
ISO/IEC TR 19583-23	Technologies de l'information – Concepts et utilisation des métadonnées – Partie 23 : Échange d'éléments de données (DEX) pour un sous-ensemble de l'ISO/IEC 11179-3
IEEE 2804	[Disponible uniquement en anglais]
ITU-T Y.3600	Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage
ISO/IEC 17913	Technologies de l'information – Cartouches de bande magnétique de 12,7mm, 128 pistes pour l'échange d'information – Format serpentant parallèle
ASTM MNL19	[Disponible uniquement en anglais]
IEEE 1636	[Disponible uniquement en anglais]
IEEE 1636.1	[Disponible uniquement en anglais]
IEEE 1636.2	[Disponible uniquement en anglais]
ISO 22600-1	INFORMATIQUE DE SANTÉ – GESTION DE PRIVILÈGES ET CONTRÔLE D'ACCÈS – PARTIE 1 : VUE D'ENSEMBLE ET GESTION DES POLITIQUES
ANSI INCITS 315	[Disponible uniquement en anglais]
ISO 10303-232	SYSTÈMES D'AUTOMATISATION INDUSTRIELLE ET INTÉGRATION – REPRÉSENTATION ET ÉCHANGE DE DONNÉES DE PRODUITS – PARTIE 232 : PROTOCOLE D'APPLICATION : INFORMATION CENTRALE ET ÉCHANGE DE PAQUETAGE DE DONNÉES TECHNIQUES
CEN/TR 16742	Systèmes de transport intelligents – Aspects de la vie privée dans les normes et les systèmes en Europe
CSA Z8002-14	Exploitation et entretien des établissements de santé
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé

CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
IEEE Std 1857.6-2018	[Disponible uniquement en anglais]
CSA Z8003	Recherche et évaluation de la conception des établissements de soins de santé

Question clé 29
portabilité et mobilité des données

BSI BS 10012 + A1	[Disponible uniquement en anglais]
BSI BS 10102-1	[Disponible uniquement en anglais]
BSI PAS 1040	[Disponible uniquement en anglais]
BSI PAS 1085	[Disponible uniquement en anglais]
BSI PAS 1296	[Disponible uniquement en anglais]
BSI PAS 183	[Disponible uniquement en anglais]
BSI PAS 185	[Disponible uniquement en anglais]
BSI PAS 1885	[Disponible uniquement en anglais]
BSI PAS 201	[Disponible uniquement en anglais]
BSI PAS 92	[Disponible uniquement en anglais]
BSI PD CEN/TR 16931-4	[Disponible uniquement en anglais]
BSI PD CEN/TR 17143	Systèmes de transport intelligents – Normes et actions nécessaires pour permettre la coordination des infrastructures urbaines en faveur des STI urbains
BSI PD CEN/TR 17475	[Disponible uniquement en anglais]
BSI PD CEN/TS 17288	[Disponible uniquement en anglais]
CEN EN 16234-1	Référentiels de e-Compétences – Référentiel européen commun pour les professionnels des technologies de l'information et de la communication dans tous les secteurs – Partie 1 : Référentiel
CEN/TS 17288	Informatique de santé – Le résumé international des patients – Lignes directrices pour la mise en œuvre européenne
CSA CSA-Q830-03	Code type sur la protection des renseignements personnels
DIN SPEC 4997	[Disponible uniquement en anglais]
DIN SPEC 91347	[Disponible uniquement en anglais]
DIN SPEC 91357	[Disponible uniquement en anglais]
DIN SPEC 91367	[Disponible uniquement en anglais]
DIN SPEC 91406	[Disponible uniquement en anglais]
DS DS/CEN/TR 17439	[Disponible uniquement en anglais]
DS DS/CEN/TR 17475	[Disponible uniquement en anglais]
DS DS/CWA 16871-1	[Disponible uniquement en anglais]
EN 319 531	[Disponible uniquement en anglais]
EN 319 532-1	[Disponible uniquement en anglais]
EN 319 532-2	[Disponible uniquement en anglais]
ETSI GR CIM 002	[Disponible uniquement en anglais]
ETSI GR ENI 007	[Disponible uniquement en anglais]

ETSI GR PDL 001	[Disponible uniquement en anglais]
ETSI GR ZSM 004	[Disponible uniquement en anglais]
ETSI GS NFV-SEC 006	[Disponible uniquement en anglais]
ETSI SR 003 381	[Disponible uniquement en anglais]
ETSI SR 003 391	[Disponible uniquement en anglais]
ETSI SR 003 392	[Disponible uniquement en anglais]
ETSI SR 003 680	[Disponible uniquement en anglais]
ETSI TR 103 305-5	[Disponible uniquement en anglais]
ETSI TR 103 370	[Disponible uniquement en anglais]
ETSI TR 103 477	[Disponible uniquement en anglais]
ETSI TR 103 509	[Disponible uniquement en anglais]
ETSI TR 103 533	[Disponible uniquement en anglais]
ETSI TR 103 534-2	[Disponible uniquement en anglais]
ETSI TR 103 536	[Disponible uniquement en anglais]
ETSI TR 103 582	Étude de cas et de communications d'utilisation impliquant des dispositifs d'IoT dans équipement de situations d'urgence
ETSI TR 103 603	[Disponible uniquement en anglais]
ETSI TR 119 500	[Disponible uniquement en anglais]
ETSI TS 102 223	[Disponible uniquement en anglais]
ETSI TS 103 458	[Disponible uniquement en anglais]
ETSI TS 103 532	[Disponible uniquement en anglais]
ETSI TS 103 643	[Disponible uniquement en anglais]
ETSI TS 132 421	[Disponible uniquement en anglais]
IEC 61800-7-202	Entraînements électriques de puissance à vitesse variable – Partie 7-202 : Interface générique et utilisation de profils pour les entraînements électriques de puissance – Spécification de profil de type 2
IEEE 1900 SERIES	[Disponible uniquement en anglais]
IEEE 1934	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
IEEE 7010	[Disponible uniquement en anglais]
IEEE NEUROTECHNOLOGIES BMI ROADMAP	[Disponible uniquement en anglais]
IEEE PHD CYBERSECURITY STANDARDS ROADMAP	[Disponible uniquement en anglais]
IEEE WHITE PAPER-0	[Disponible uniquement en anglais]
ISO 10617	Textiles – Format de données standard pour la communication colorimétrique – Textiles et mesurages associés
ISO 10667-2	LIVRAISON D'UN SERVICE D'ÉVALUATION – MODES OPÉRATOIRES ET MÉTHODES D'ÉVALUATION DES PERSONNES AU TRAVAIL ET DES PARAMÈTRES ORGANISATIONNELS – PARTIE 2 : EXIGENCES POUR LES FOURNISSEURS DE SERVICE
ISO 13606-4	Informatique de santé – Communication du dossier de santé informatisé – Partie 4 : Sécurité
ISO 17115	[Disponible uniquement en anglais]
ISO 17117-1	Informatique de santé – Ressources terminologiques – Partie 1 : Caractéristiques

ISO 18308	Informatique de santé – Exigences relatives à une architecture de l'enregistrement électronique en matière de santé
ISO 18750	SYSTÈME DE TRANSPORTS INTELLIGENTS – SYSTÈMES COOPÉRATIFS – CARTE LOCALE DYNAMIQUE
ISO 19465	Médecine traditionnelle chinoise – Catégories de systèmes terminologiques de médecine traditionnelle chinoise (MTC) clinique
ISO 19626-1	Processus, éléments d'informations et documents dans le commerce, l'industrie et l'administration – Plates-formes de communication sécurisées pour documents électroniques – Partie 1 : Généralités
ISO 20264	Émissions de sources fixes – Détermination de la concentration en masse de composés organiques volatils (COV) individuels dans les gaz résiduaires issus de processus sans combustion
ISO 22367	Laboratoires de biologie médicale – Application de la gestion des risques aux laboratoires de biologie médicale
ISO 23354	TITRE MANQUE
ISO 25237	Informatique de santé – Pseudonymisation
ISO 26000	LIGNES DIRECTRICES RELATIVES À LA RESPONSABILITÉ SOCIÉTALE
ISO 37156	INFRASTRUCTURES URBAINES INTELLIGENTES – CADRE DIRECTEUR POUR L'ÉCHANGE ET LE PARTAGE DE DONNÉES POUR LES INFRASTRUCTURES URBAINES INTELLIGENTES
ISO IWA 31	Management du risque – Lignes directices pour l'utilisation de l'ISO 31000 dans les systèmes de management
ISO TR 24971	Dispositifs médicaux – Recommandations relatives à l'application de l'ISO 14971
ISO TS 16843-1	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 1 : Points d'acupuncture
ISO TS 16843-2	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 2 : Puncture
ISO TS 16843-3	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 3 : Moxibustion
ISO TS 16843-4	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 4 : Les méridiens et leurs collatéraux
ISO TS 16843-5	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 5 : N/A
ISO TS 18101-1	Systèmes d'automatisation et intégration – Interopérabilité entre les industries du pétrole et du gaz – Partie 1 : Vue d'ensemble et principes fondamentaux
ISO TS 18790-1	Informatique de santé – Cadre de profilage et classification pour le développement de normes informatiques relatives à la médecine chinoise – Partie 1 : Médecine chinoise traditionnelle
ISO TS 19299	PERCEPTION DE TÉLÉPÉAGE – CADRE DE SÉCURITÉ
ISO TS 19844	INFORMATIQUE DE SANTÉ – IDENTIFICATION DES MÉDICAMENTS – LIGNES DIRECTRICES POUR·LA·MISE·EN·OEUVRE DE L'ISO 11238 RELATIVE AUX ÉLÉMENTS DE DONNÉES ET STRUCTURES POUR L'IDENTIFICATION UNIQUE ET L'ÉCHANGE D'INFORMATIONS RÉGLEMENTÉES SUR LES SUBSTANCES
ISO TS 21192	Perception du télépéage – Aide pour la gestion du trafic
ISO TS 21547	INFORMATIQUE DE SANTÉ – EXIGENCES DE SÉCURITÉ POUR L'ARCHIVAGE DES DOSSIERS DE SANTÉ ÉLECTRONIQUES – PRINCIPES
ISO TS 21831	[Disponible uniquement en anglais]
ISO TS 22773	[Disponible uniquement en anglais]
ISO TS 22789	Informatique de santé – Cadre conceptuel pour les constats des patients et les problèmes de terminologies
ISO TS 22835	[Disponible uniquement en anglais]
ISO TS 22990	[Disponible uniquement en anglais]
ISO TS 23303	[Disponible uniquement en anglais]

ISO TS 8000-311	QUALITÉ DES DONNÉES – PARTIE 311 : DIRECTIVES POUR L'APPLICATION DE LA QUALITÉ DES DONNÉES DE PRODUIT POUR LES FORMES (PDQ-S)
ISO/IEC 12087-5	TECHNOLOGIES DE L'INFORMATION – INFOGRAPHIE ET TRAITEMENT DE L'IMAGE – SPÉCIFICATION FONCTIONNELLE POUR LE TRAITEMENT DE L'IMAGE ET L'ÉCHANGE (IPI) – PARTIE 5 : FORMAT D'ÉCHANGE DE L'IMAGE DE BASE (BIIF)
ISO/IEC 15944-12	Technologies de l'information – Vue opérationnelle d'affaires – Partie 12 : Exigences en matière de protection de la vie privée (PPR) relatives à la gestion du cycle de vie de l'information (ILCM) et de l'EDI des renseignements personnels (PI)
ISO/IEC 17789	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – ARCHITECTURE DE RÉFÉRENCE
ISO/IEC 18384-2	TECHNOLOGIE DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE POUR L'ARCHITECTURE ORIENTÉE SERVICE (SOA RA) – PARTIE 2 : ARCHITECTURE DE RÉFÉRENCE POUR LES SOLUTIONS DE L'ARCHITECTURE ORIENTÉE SERVICE
ISO/IEC 19086-1	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 1 : APERÇU GÉNÉRAL ET CONCEPTS
ISO/IEC 19086-3	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – CADRE DE TRAVAIL DE L'ACCORD DU NIVEAU DE SERVICE – PARTIE 3 : EXIGENCES DE CONFORMITÉ ESSENTIELLES
ISO/IEC 19286	CARTES D'IDENTIFICATION – CARTES À CIRCUIT INTÉGRÉ – PROTOCOLES ET SERVICES RENFORÇANT LA PROTECTION DES DONNÉES PERSONNELLES
ISO/IEC 19780-1	Technologies de l'information – Apprentissage, éducation et formation – Technologie collaborative – Communication d'apprentissage collaboratif – Partie 1 : Communication à base de texte
ISO/IEC 19941	TECHNOLOGIES DE L'INFORMATION – INFORMATIQUE EN NUAGE – INTEROPÉRABILITÉ ET PORTABILITÉ
ISO/IEC 19944	INFORMATIQUE EN NUAGE ET PLATES-FORMES DISTRIBUÉES – FLUX DE DONNÉES, CATÉGORIES DE DONNÉES ET UTILISATION DES DONNÉES – PARTIE 1 : PRINCIPES DE BASE
ISO/IEC 20748.2	TECHNOLOGIES DE L'INFORMATION – ÉDUCATION, FORMATION ET APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 2 : EXIGENCES RELATIVES AU SYSTÈME
ISO/IEC 21964-1	Technologies de l'information – Destruction de véhicules de données – Partie 1 : Principes et concepts
ISO/IEC 21964-3	Technologies de l'information – Destruction de véhicules de données – Partie 3 : Processus de destruction des supports de données
ISO/IEC 22624	[Disponible uniquement en anglais]
ISO/IEC 27701	TECHNIQUES DE SÉCURITÉ – EXTENSION D'ISO/IEC 27001 ET ISO/IEC 27002 AU MANAGEMENT DE LA PROTECTION DE LA VIE PRIVÉE – EXIGENCES ET LIGNES DIRECTRICES
ISO/IEC 29184	TECHNOLOGIES DE L'INFORMATION – DÉCLARATIONS DE CONFIDENTIALITÉ EN LIGNE ET LES CONSENTEMENTS
ISO/IEC 38505.2	TECHNOLOGIES DE L'INFORMATION – GOUVERNANCE DES TECHNOLOGIES DE L'INFORMATION – PARTIE 2 : IMPLICATIONS DE L'ISO/IEC 38505-1 POUR LA GESTION DES DONNÉES
ISO/IEC GUIDE 71	Guide pour l'intégration de l'accessibilité dans les normes
ISO/IEC TR 20547-2	TECHNOLOGIES DE L'INFORMATION – ARCHITECTURE DE RÉFÉRENCE DES BIG DATA – PARTIE 2 : CAS PRATIQUES ET EXIGENCES DÉRIVÉES
ISO/IEC TR 20748-2	TECHNOLOGIES DE L'INFORMATION – ÉDUCATION, FORMATION ET APPRENTISSAGE – INTEROPÉRABILITÉ DE L'ANALYTIQUE DE L'APPRENTISSAGE – PARTIE 2 : EXIGENCES RELATIVES AU SYSTÈME
ISO/IEC TR 22678	[Disponible uniquement en anglais]
ISO/IEC TR 23186	[Disponible uniquement en anglais]
ISO/IEC TR 27550	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – INGÉNIERIE DE LA VIE PRIVÉE POUR LES PROCESSUS DU CYCLE DE VIE DES SYSTÈMES
ISO/IEC TR 30164	L'INTERNET DES OBJETS (IOT) – INFORMATIQUE EN PÉRIPHÉRIE
ISO/IEC TR 38505-2	Technologies de l'information – Gouvernance des technologies de l'information – Partie 2 : Implications de l'ISO/IEC 38505-1 pour la gestion des données

ISO/IEC TS 20748-4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4 :
ISO/IEC/IEEE 8802-1AX	Technologies de l'information – Télécommunications et échange d'information entre systèmes – Réseaux locaux et métropolitains – Exigences spécifiques – Partie 1AX : Agrégation de lien
ISO/TR 17427-7	Systèmes intelligents de transport – Systèmes intelligents de transport coopératifs – Partie 7 : Aspects relatifs à la vie privée
ISO/TR 23021	[Disponible uniquement en anglais]
ISO/TR 23022	Médecine traditionnelle chinoise – Vocabulaire contrôlé relatif aux formules Kampo japonaises et codes d'indication des produits
ISO/TR 24971	Dispositifs médicaux – Recommandations relatives à l'application de l'ISO 14971
ISO/TS 14441	Informatique de santé – Sécurité et exigences d'intimité des systèmes de EHR pour l'évaluation de la conformité
ISO/TS 16277-1	Informatique de santé – Structures catégorielles des recherches cliniques en médecine traditionnelle – Partie 1 : Médecine traditionnelle de l'Asie de l'est
ISO/TS 16843-1	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 1 : Points d'acupuncture
ISO/TS 16843-3	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 3 : Moxibustion
ISO/TS 16843-4	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 4 : Les méridiens et leurs collatéraux
ISO/TS 16843-5	Informatique de santé – Structures catégoriques pour la représentation de l'acupuncture – Partie 5 : N/A
ISO/TS 18062	Informatique de santé – Structure catégorielle pour la représentation de médicaments à base de plantes dans les systèmes terminologiques
ISO/TS 18101-1	Systèmes d'automatisation et intégration – Interopérabilité entre les industries du pétrole et du gaz – Partie 1 : Vue d'ensemble et principes fondamentaux
ISO/TS 18750	Système de transports intelligents – Systèmes coopératifs – Carte locale dynamique
ISO/TS 18790-1	Informatique de santé – Cadre de profilage et classification pour le développement de normes informatiques relatives à la médecine chinoise – Partie 1 : Médecine chinoise traditionnelle
ISO/TS 21192	Perception du télépéage – Aide pour la gestion du trafic
ISO/TS 21564	[Disponible uniquement en anglais]
ISO/TS 21831	[Disponible uniquement en anglais]
ISO/TS 22773	[Disponible uniquement en anglais]
ISO/TS 22835	[Disponible uniquement en anglais]
ISO/TS 23303	[Disponible uniquement en anglais]
ITU-R M.1457-14	[Disponible uniquement en anglais]
ITU-T G.1032	Facteurs ayant une influence sur la qualité de l'expérience de jeu
ITU-T K.81	Guide sur l'immunité des systèmes de télécommunication aux attaques électromagnétiques de haute puissance
ITU-T L.1305	Système de gestion de l'infrastructure des centres de données fondé sur les mégadonnées et l'intelligence artificielle
ITU-T L.1470	Trajectoires des émissions de gaz à effet de serre pour le secteur des technologies de l'information et de la communication compatibles avec l'Accord de Paris adopté par la CCNUCC
ITU-T SERIES H SUPP 17	[Disponible uniquement en anglais]
ITU-T SERIES Q SUPP 65	[Disponible uniquement en anglais]
ITU-T SERIES Q SUPP 66	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 49	[Disponible uniquement en anglais]

ITU-T SERIES Y SUPP 52	[Disponible uniquement en anglais]
ITU-T SERIES Y SUPP 56	[Disponible uniquement en anglais]
ITU-T Y.3052	Aperçu de l'instauration de la confiance dans les infrastructures et les services des technologies de l'information et de la communication
ITU-T Y.3173	Cadre pour l'évaluation des niveaux d'intelligence des réseaux futurs, y compris les IMT-2020
ITU-T Y.3502	Technologies de l'information – Informatique en nuage – Architecture de référence
ITU-T Y.4003	Aperçu de la fabrication intelligente dans le contexte de l'Internet des objets industriel
ITU-T Y.4905	Évaluation de l'impact des villes intelligentes et durables
ITU-T Y.4906	Cadre d'évaluation de la transformation numérique des secteurs dans les villes intelligentes
SAE AIR6904	[Disponible uniquement en anglais]
SAE AS5506C	[Disponible uniquement en anglais]
SAE R-463	[Disponible uniquement en anglais]
AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-2:2020	Gouvernance Des Données – Partie 2 : Accès de tiers aux données
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CSA Z8003	Recherche et évaluation de la conception des établissements de soins de santé

Groupe de travail 4 : Analyses, solutions et commercialisation

Question clé 30 éléments techniques des solutions d'IA

ANSI INCITS 172	[Disponible uniquement en anglais]
ANSI X9.112-3	[Disponible uniquement en anglais]
API PUBL 4452	[Disponible uniquement en anglais]
ASCE 70-19	[Disponible uniquement en anglais]
ASCE GSP 199	[Disponible uniquement en anglais]
ASCE GSP 318	[Disponible uniquement en anglais]
ASHRAE 4692	[Disponible uniquement en anglais]
ASHRAE AB-10-022	[Disponible uniquement en anglais]
ASHRAE DATACOM SERIES BOOK 14	[Disponible uniquement en anglais]
ASHRAE TRAN 2010-2	[Disponible uniquement en anglais]
ASHRAE TRAN 2019-2	[Disponible uniquement en anglais]

ASHRAE TRAN 2020-1	[Disponible uniquement en anglais]
ASTM F2446	[Disponible uniquement en anglais]
ASTM F3060	[Disponible uniquement en anglais]
BSI BS 10008-2	[Disponible uniquement en anglais]
BSI BS 10102-1	[Disponible uniquement en anglais]
BSI BS 5192-1	[Disponible uniquement en anglais]
BSI PAS 1000	[Disponible uniquement en anglais]
BSI PAS 1040	[Disponible uniquement en anglais]
BSI PAS 1085	[Disponible uniquement en anglais]
BSI PAS 1880	[Disponible uniquement en anglais]
BSI PAS 1885	[Disponible uniquement en anglais]
BSI PAS 440	[Disponible uniquement en anglais]
BSI PAS 7040	[Disponible uniquement en anglais]
BSI PAS 7340	[Disponible uniquement en anglais]
CIE X046 VOL 1-2	[Disponible uniquement en anglais]
DS DS/CWA 17492	[Disponible uniquement en anglais]
DIN SPEC 92001-1	[Disponible uniquement en anglais]
ETSI EG 202 301	[Disponible uniquement en anglais]
ETSI EN 303 470	[Disponible uniquement en anglais]
ETSI ES 202 336-12	[Disponible uniquement en anglais]
ETSI GR ARF 002	[Disponible uniquement en anglais]
ETSI GR CIM 002	[Disponible uniquement en anglais]
ETSI GR ENI 003	[Disponible uniquement en anglais]
ETSI GR ENI 004	[Disponible uniquement en anglais]
ETSI GR ENI 007	[Disponible uniquement en anglais]
ETSI GR ZSM 004	[Disponible uniquement en anglais]
ETSI GS ENI 001	[Disponible uniquement en anglais]
ETSI GS ENI 002	[Disponible uniquement en anglais]
ETSI GS ENI 005	[Disponible uniquement en anglais]
ETSI GS MEC 002	[Disponible uniquement en anglais]
ETSI GS ZSM 001	[Disponible uniquement en anglais]
ETSI GS ZSM 002	[Disponible uniquement en anglais]
ETSI GS ZSM 007	[Disponible uniquement en anglais]
ETSI SR 003 680	[Disponible uniquement en anglais]
ETSI TR 102 647	[Disponible uniquement en anglais]
ETSI TR 102 659-1	[Disponible uniquement en anglais]
ETSI TR 103 077	[Disponible uniquement en anglais]
ETSI TR 103 306	[Disponible uniquement en anglais]
ETSI TR 103 438	[Disponible uniquement en anglais]
ETSI TR 103 508	[Disponible uniquement en anglais]

ETSI TR 103 534-2	[Disponible uniquement en anglais]
ETSI TR 103 536	[Disponible uniquement en anglais]
ETSI TR 103 562	[Disponible uniquement en anglais]
ETSI TR 103 582	Étude de cas et de communications d'utilisation impliquant des dispositifs d'IoT dans équipement de situations d'urgence
ETSI TR 103 603	[Disponible uniquement en anglais]
ETSI TR 103 626	[Disponible uniquement en anglais]
ETSI TR 103 644	[Disponible uniquement en anglais]
ETSI TS 103 195-2	[Disponible uniquement en anglais]
ETSI TS 103 300-2	[Disponible uniquement en anglais]
ETSI TS 105 174-8	[Disponible uniquement en anglais]
IEC 60050-171	Vocabulaire Electrotechnique International (IEV) – Partie 171 : Technologies numériques – Concepts fondamentaux
IEC 60194	Conception, fabrication et assemblage des cartes imprimées – Termes et définitions
IEC 61508 SET REDLINE	Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité
IEC 61508-7	Sécurité fonctionnelle des systèmes électriques / électroniques / électroniques programmables relatifs à la sécurité – Partie 7 : Présentation de techniques et mesures
IEC 62243	[Disponible uniquement en anglais]
IEEE 1484.1	[Disponible uniquement en anglais]
IEEE 1636	[Disponible uniquement en anglais]
IEEE 1671.1	[Disponible uniquement en anglais]
IEEE 1900 SERIES	[Disponible uniquement en anglais]
IEEE 1900.1	[Disponible uniquement en anglais]
IEEE 1934	[Disponible uniquement en anglais]
IEEE 2413	[Disponible uniquement en anglais]
IEEE 2430	[Disponible uniquement en anglais]
IEEE 24765	[Disponible uniquement en anglais]
IEEE 2755.1	[Disponible uniquement en anglais]
IEEE 7010	[Disponible uniquement en anglais]
IEEE 802.22	[Disponible uniquement en anglais]
IEEE NEUROTECHNOLOGIES BMI ROADMAP	[Disponible uniquement en anglais]
IEEE WHITE PAPER 3DBP IC	[Disponible uniquement en anglais]
IEEE WHITE PAPER-0	[Disponible uniquement en anglais]
ISO 16355-3	Application des méthodes statistiques et des méthodes liées aux nouvelles technologies et de développement de produit – Partie 3 : Acquisition quantitative du retour client (voice of customer) ou du retour des parties prenantes (voice of stakholders)
ISO 24617-1	Gestion des ressources langagières – Cadre d'annotation sémantique (SemAF) – Partie 1 : Temps et événements (SemAF-Time, ISO-TimeML)
ISO 24617-7	Gestion des ressources linguistiques – Cadre d'annotation sémantique – Partie 7 : Information spatiale
ISO 9409-1	Robots manipulateurs industriels – Interfaces mécaniques – Partie 1 : Interfaces à plateau

ISO IWA 31	Management du risque – Lignes directrices pour l'utilisation de l'ISO 31000 dans les systèmes de management
ISO TR 23455	[Disponible uniquement en anglais]
ISO/IEC 11179-1	TECHNOLOGIES DE L'INFORMATION – REGISTRES DE MÉTADONNÉES (RM) – PARTIE 1 : CADRE DE RÉFÉRENCE
ISO/IEC 19788-3	Technologies de l'information – Apprentissage, éducation et formation – Métadonnées pour ressources d'apprentissage – Partie 3 : Profil d'application de base
ISO/IEC 20748.4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4 :
ISO/IEC 23001-4	Technologies de l'information – Technologies des systèmes MPEG – Partie 4 : Représentation de configuration codec
ISO/IEC 2382-1	Technologies de l'information – Vocabulaire – Partie 1 : Termes fondamentaux
ISO/IEC 27021	TECHNOLOGIES DE L'INFORMATION – TECNIQUES DE SÉCURITÉ – EXIGENCES DE COMPÉTENCE POUR LES PROFESSIONNELS DE LA GESTION DES SYSTÈMES DE MANAGEMENT DE LA SÉCURITÉ
ISO/IEC TR 23188	[Disponible uniquement en anglais]
ISO/IEC TR 24741	TECHNOLOGIES DE L'INFORMATION – BIOMÉTRIE – APERÇU GÉNÉRAL ET APPLICATIONS
ISO/IEC TR 27550	TECHNOLOGIES DE L'INFORMATION – TECHNIQUES DE SÉCURITÉ – INGÉNIERIE DE LA VIE PRIVÉE POUR LES PROCESSUS DU CYCLE DE VIE DES SYSTÈMES
ISO/IEC TS 20748-4	Technologies pour l'éducation, la formation et l'apprentissage – interopérabilité de l'analytique de l'apprentissage – Partie 4 :
ISO/TR 23455	[Disponible uniquement en anglais]
ISO/TR 23845	[Disponible uniquement en anglais]
ISO/TS 22287	[Disponible uniquement en anglais]
ITU-T F.749.10	Exigences pour les services de communication pour les aéronefs sans pilote civils
ITU-T L.1022	Économie circulaire : définitions et concepts relatifs à l'efficacité de l'utilisation des matériaux pour les technologies de l'information et de la communication
ITU-T L.1305	Système de gestion de l'infrastructure des centres de données fondé sur les mégadonnées et l'intelligence artificielle
ITU-T L.1380	Solution intelligente en matière d'énergie pour les sites de télécommunication
ITU-T M.3041	Cadre pour l'exploitation, la gestion et la maintenance intelligentes
ITU-T Q.1200	Structure des Recommandations de la série Q sur le réseau intelligent
ITU-T SERIES K SUPP 16	[Disponible uniquement en anglais]
ITU-T Y.3101	Exigences relatives aux réseaux IMT-2020
ITU-T Y.3173	Cadre pour l'évaluation des niveaux d'intelligence des réseaux futurs, y compris les IMT-2020
ITU-T Y.3324	Exigences et cadre architectural pour la gestion et le contrôle autonomes des réseaux IMT-2020
ITU-T Y.3508	Informatique en nuage – Aperçu et exigences de haut niveau pour l'informatique en nuage répartie
ITU-T Y.3800	Aperçu des réseaux prenant en charge la distribution de clés quantiques
ITU-T Y.4003	Aperçu de la fabrication intelligente dans le contexte de l'Internet des objets industriel
ITU-T Y.4204	Exigences en matière d'accessibilité pour les applications et les services de l'Internet des objets
ITU-T Y.4904	Modèle de maturité pour les villes intelligentes et durables
ITU-T Y.4906	Cadre d'évaluation de la transformation numérique des secteurs dans les villes intelligentes
NEMA IOT P2	[Disponible uniquement en anglais]
SAE AIR1266A	[Disponible uniquement en anglais]

SAE ARP5150A	[Disponible uniquement en anglais]
SAE ARP6407	[Disponible uniquement en anglais]
SAE PT-202	[Disponible uniquement en anglais]
SAE PT-204	[Disponible uniquement en anglais]
SAE PT-205	[Disponible uniquement en anglais]
SAE PT-207	[Disponible uniquement en anglais]
SAE R-441	[Disponible uniquement en anglais]
SAE R-463	[Disponible uniquement en anglais]
UL 4600	[Disponible uniquement en anglais]

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

IMDRF/SaMD WG/ N10FINAL:201	[Disponible uniquement en anglais]
IMDRF/SaMD WG/ N12FINAL:2014	[Disponible uniquement en anglais]
IMDRF/SaMD WG/N23 FINAL:2015	[Disponible uniquement en anglais]
N/A	Ligne Directrice : Logiciels à titre d'instruments médicaux : Définition et Classification
N/A	[Disponible uniquement en anglais]
ISO/IEC DTR 29119-11	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 101:2019	Intelligence artificielle : Conception éthique et utilisation de systèmes de décision automatisés
CAN/CIOSC 107	Essais et bancs d'essai pour les véhicules autonomes
IEEE P1232.3/D3.2	[Disponible uniquement en anglais]

Question clé 31
chaîne de valeur des données

ETSI TR 103 376	[Disponible uniquement en anglais]
ITU-T Y.3601	Mégadonnées – Cadre et exigences pour l'échange de données
ETSI TR 103 305-5	[Disponible uniquement en anglais]
ETSI TR 103 534-2	[Disponible uniquement en anglais]
ETSI TR 103 603	[Disponible uniquement en anglais]
IEEE 1232.1	[Disponible uniquement en anglais]

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

N/A	[Disponible uniquement en anglais]
N/A	Étude : La valeur des données au Canada : estimations expérimentales
N/A	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données

CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 100-8	Gouvernance des données-Partie 8 : Cadre de géorésidence et de souveraineté
IEEE IC18-004	[Disponible uniquement en anglais]

Question clé 32
transparence et communication de l'analyse des données

ISO/IEC TR 24028	TECHNOLOGIES DE L'INFORMATION – INTELLIGENCE ARTIFICIELLE – EXAMEN D'ENSEMBLE DE LA FIABILITÉ EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
ISO/IEC 20889:2018	TERMINOLOGIE ET CLASSIFICATION DES TECHNIQUES DE DÉ-IDENTIFICATION DE DONNÉES POUR LA PROTECTION DE LA VIE PRIVÉE
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL
n/a	Évaluation de l'incidence algorithmique
n/a	Données ouvertes
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-1:2020	Gouvernance Des Données – Partie 1 : Protection des données des actifs numériques
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-8	Gouvernance des données-Partie 8 : Cadre de géorésidence et de souveraineté
IEEE P7001	[Disponible uniquement en anglais]
IEEE IC18-004	[Disponible uniquement en anglais]

Question clé 33
interprétabilité et explicabilité des systèmes d'IA

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL

n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]

n/a	RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL
ISO/IEC DTR 29119-11	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
ISO/IEC TR 24028:2020	TECHNOLOGIES DE L'INFORMATION – INTELLIGENCE ARTIFICIELLE – EXAMEN D'ENSEMBLE DE LA FIABILITÉ EN MATIÈRE D'INTELLIGENCE ARTIFICIELLE
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 101:2019	Intelligence artificielle : Conception éthique et utilisation de systèmes de décision automatisés
IEEE P2894	[Disponible uniquement en anglais]

Question clé
34 évaluation et gestion des biais

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO/IEC AWI TR 24027	[Disponible uniquement en anglais]
IEEE P7003	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada
CAN/CIOSC 100-3	Gouvernance des données – Partie 3 : Cadre de désidentification des données améliorant la confidentialité
CAN/CIOSC 100-6	Gouvernance des données – Partie 6 : Collecte et utilisation responsables des données de traçage et de surveillance des contacts numériques sur le lieu de travail
CAN/CIOSC 100-7	Gouvernance des données – Partie 7 : gérance responsable des données
CAN/CIOSC 101:2019	Intelligence artificielle : Conception éthique et utilisation de systèmes de décision automatisés
IEEE P7003	[Disponible uniquement en anglais]
N/A	[Disponible uniquement en anglais]

Question clé
35 gestion de la performance de l'analyse et de systèmes d'IA

AUTRES DOCUMENTS D'ORIENTATION/NORMES PROPOSÉS PAR LES MEMBRES DU GROUPE DE TRAVAIL	
ISO/IEC 38507	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
n/a	[Disponible uniquement en anglais]
CAN/CIOSC 100-n	Série de normes sur la gouvernance des données
CAN/CIOSC 100-5	Gouvernance des données – Partie 5 : Cadre de capacité des données et des informations sur la santé
CAN/CIOSC 111-x	Série de normes favorisant la mise en place d'un système de scrutin électoral en ligne au Canada

Annexe C –

Consultations autochtones sur les travaux du CCNGD

Consultation autochtone sur les travaux du Collectif canadien de normalisation en matière de gouvernance des données – Premières perspectives sur les enjeux de la gouvernance des données

Nous remercions les personnes qui ont répondu au sondage et participé aux entrevues pour leurs commentaires, conseils et points de vue sur la gouvernance des données. Ce rapport n'aurait pas pu voir le jour sans leur aide et leur expertise.

Souveraineté des données autochtones

Il importe de mettre d'emblée en contexte l'utilisation du terme « souveraineté des données autochtones » dans le présent rapport. Au Canada, l'adjectif « autochtone » renvoie aux Premières Nations, aux Inuits et aux Métis. Il est essentiel de reconnaître que la souveraineté des données représente non pas une approche panautochtone adoptée par tous, mais plutôt une approche définie et dirigée par les Premières Nations, les Inuits et les Métis. En utilisant le terme « souveraineté des données autochtones » dans le présent rapport, nous faisons référence aux efforts déployés collectivement par les Premières Nations, les Inuits et les Métis pour atteindre la souveraineté des données dans le respect de leurs lois, de leurs cultures, de leurs protocoles et de leurs visions du monde.

Rédaction
Firelight Research Inc.

Table des matières

Sommaire

Le Conseil canadien des normes a confié à Firelight le mandat de concevoir, de préparer, d'administrer, d'organiser virtuellement et d'animer une première consultation autochtone dans l'ensemble du pays dans le but d'intégrer les points de vue autochtones sur la gouvernance des données au Canada à la préparation de la feuille de route du Collectif canadien de normalisation en matière de gouvernance des données (CCNGD). Cette consultation consistait en un sondage en ligne et des entrevues avec les principaux participants. Dans le présent rapport, nous mettons en contexte les enjeux liés à la gouvernance et à la souveraineté des données autochtones avant de résumer les résultats des consultations et de formuler des recommandations à partir des commentaires des participants. Ces derniers nous ont autorisés à utiliser leurs réponses avant de répondre au sondage ou de participer à l'entrevue.

Tout peuple a besoin de données de haute qualité sur sa population, ses communautés, son territoire, ses ressources et sa culture pour prendre des décisions éclairées, et les peuples autochtones (c'est-à-dire les Premières Nations, les Inuits et les Métis du Canada) ne font pas exception. Pourtant, ces peuples et leurs instances dirigeantes peinent toujours à obtenir leur autonomie en matière de gouvernance des données. Depuis longtemps, la collecte et la gestion des données sur les communautés autochtones sont principalement effectuées par des organismes externes; en l'absence d'un leadership autochtone, elles ne reflètent ni les priorités, ni les besoins, ni les visions du monde, ni les valeurs des communautés autochtones. Les données sont donc extraites des communautés, les indicateurs servant à mesurer la santé et le bien-être sont inadéquats, et les données sur les peuples autochtones sont mal utilisées. C'est dans ce contexte qu'émerge la notion de souveraineté des données autochtones, c'est-à-dire le droit d'une instance dirigeante autochtone de diriger la collecte, la propriété, la diffusion et l'application de ses propres données sur ses communautés, ses membres, ses terres et ses ressources. Les données autochtones représentent un aspect important de la souveraineté autochtone dans son ensemble, et du mouvement vers l'autonomie gouvernementale, l'autodétermination et la décolonisation.

Dans une première étape, la consultation a pris la forme d'un sondage en ligne pour joindre le plus de monde possible dans les délais prévus. Ce sondage visait à recueillir des commentaires sur la nature et l'importance, dans un contexte autochtone, de dix enjeux définis par le groupe de travail 1. Le sondage a été mené en anglais et en français du 12 janvier au 2 février 2021. Au total, 36 personnes ont répondu à la version anglaise, et aucune à la version française. On leur a demandé de classer en ordre d'importance dix enjeux des fondements de la gouvernance des données : ce sont les *directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique*, le *cadre des responsabilités* et la *gouvernance de la gestion des données* qui ont été le plus fréquemment jugés « très importants » dans l'élaboration de normes sur la gouvernance des données. Aucun des enjeux n'a été jugé sans importance. Les résultats du sondage figurent à la section 4.1, et le tableau 3 résume les commentaires des participants sur chaque enjeu.

Nous avons mené des entrevues auprès de praticiens et d'experts en gouvernance des données des Premières Nations, des Inuits et des Métis pour mieux comprendre les points de vue autochtones sur ces enjeux. Les participants ont été choisis en fonction de leur expertise et de leur expérience au sein d'organisations ou dans le cadre de projets et d'initiatives axés sur la gouvernance des données autochtones. Nous nous sommes efforcés de recruter des experts des différents contextes propres aux Premières Nations, aux Inuits et aux Métis, dans l'ensemble du Canada. Environ la moitié des personnes invitées à une entrevue ont été en mesure d'y participer. Au total, 12 personnes ont été interrogées dans le cadre de huit entrevues. On trouvera la liste des principaux participants à la section 3.3.

Voici les grands enjeux de gouvernance des données autochtones qui se dégagent de l'analyse thématique des réponses au sondage et aux entrevues :

- Reconnaissance de l'autorité : L'autorité souveraine des gouvernements autochtones sur tous les aspects du cycle de vie des données relatives à leur population, leurs terres et leurs eaux n'est pas reconnue.
- Capacité : La capacité des gouvernements et organisations autochtones de diriger la collecte, la gestion, la conservation et la communication des données a été décrite en termes d'infrastructures, d'équipements, de ressources humaines, de formation, de technologie et de financement.
- Accès aux données : Les gouvernements et organisations autochtones n'ont souvent pas accès à l'information dont ils ont besoin sur leurs populations et sur les terres et les eaux qu'ils administrent. Cette information étant hébergée par des chercheurs, des gouvernements ou d'autres organisations, les décideurs autochtones manquent des données nécessaires pour gouverner.
- Respect de la culture : Les données doivent être recueillies par des organisations autochtones, et les méthodes de collecte et de gestion de ces données doivent refléter le contexte culturel, les valeurs et les normes autochtones propres à chaque projet.

Si le présent rapport peut être considéré comme un premier compte-rendu des perspectives autochtones sur les enjeux de gouvernance des données et les manières possibles de s'y attaquer, il comporte un certain nombre de limites dont il faut tenir compte dans l'interprétation des résultats : seul un petit nombre de représentants d'organisations inuites et métisses ont répondu à la consultation; par ailleurs, étant donné les contraintes temporelles et budgétaires, il n'était pas possible d'aborder en détail chacun des 35 enjeux définis par les groupes de travail du CCNGD. Ces limites sont précisées à la section 1.3.

Les participants ont signalé l'existence de principes, normes et initiatives directement pertinents pour l'élaboration de normes sur la gouvernance des données. Ils affirment la souveraineté des peuples autochtones sur tous les aspects de la collecte, de la gestion et de l'utilisation des données. Il s'agit des principes de PCAP® des Premières Nations, de la Stratégie de gouvernance des données des Premières Nations (SGDPN) et de la Stratégie nationale inuite sur la recherche (SNIR); ils sont présentés à la section 4.3.

Dans la section 5, nous formulons des recommandations basées sur les commentaires recueillis quant à la consultation et à la participation des gouvernements et organisations autochtones tout au long du processus du CCNGD :

1. Impliquer davantage les organisations et les experts en gouvernance des données inuits et métis. Étant donné leur faible participation à la consultation, il faut poursuivre les travaux pour connaître le point de vue de ces importants groupes autochtones sur les questions de gouvernance des données et sur les travaux du CCNGD.
2. Impliquer davantage les gouvernements et organisations autochtones dans le processus du CCNGD pour consacrer suffisamment de temps et de ressources à une définition claire des enjeux soulevés par les gouvernements et organisations autochtones et à leur intégration, le cas échéant, aux enjeux déjà définis par les groupes de travail du CCNGD. Cela peut notamment se traduire par la participation de représentants autochtones aux groupes de travail du CCNGD. Par exemple, un certain nombre d'enjeux définis par le groupe de travail 1 qui ont obtenu un classement élevé au sondage, dont les *directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique*, le *cadre des responsabilités* et la *gouvernance de la gestion des données*, devront faire l'objet d'une rétroaction supplémentaire de la part des gouvernements et organisations autochtones.
3. Au moyen d'autres consultations, repérer les principales organisations autochtones (notamment celles qui s'occupent déjà d'élaborer des normes ou des principes, comme l'Inuit Tapiriit Kanatami et le Centre de gouvernance de l'information des Premières Nations) en vue de les impliquer dans les prochaines étapes des travaux du CCNGD, y compris la normalisation elle-même.

1. Introduction

1.1 RÉSUMÉ

Nous présentons ici les résultats d'une première consultation autochtone sur les enjeux de gouvernance de données, réalisée pour le Collectif canadien de normalisation en matière de gouvernance des données (CCNGD). Soulignons d'entrée de jeu que ce rapport ne prétend ni constituer la somme des perspectives autochtones sur le sujet, ni refléter tous les points de vue des Premières Nations, des Inuits et des Métis. La section 1.3 donne des précisions sur les limites de la consultation et des données recueillies. La suite du processus du CCNGD devra prévoir un dialogue constant avec les gouvernements et organisations autochtones pour assurer une participation et un leadership autochtones pendant l'élaboration et l'application de toute norme ou initiative découlant de ce processus.

La gouvernance des données revêt une importance particulière, collectivement et individuellement, pour les communautés des Premières Nations, des Inuits et des Métis. Pour situer le contexte des contributions et commentaires recueillis pendant les premières consultations autochtones, la section 2 décrit les particularités de la gouvernance des données autochtones et ses liens avec les répercussions passées et présentes de la colonisation, avant de présenter une brève analyse de la contribution des processus de décolonisation et d'autodétermination autochtones à la promotion de la souveraineté des données. La section 3 présente un sommaire des méthodes de consultation, alors que les résultats – accompagnés des principaux enjeux soulevés lors des consultations – figurent à la section 4. Des recommandations basées sur les réponses recueillies sont présentées à la section 5.

1.2 PORTÉE DES TRAVAUX

Le Conseil canadien des normes a confié à Firelight le mandat de concevoir, de préparer, d'administrer, d'organiser virtuellement et d'animer une première consultation autochtone dans l'ensemble du pays dans le but d'intégrer les points de vue autochtones sur la gouvernance des données au Canada à la préparation de la feuille de route du CCNGD.

Voici l'essentiel du mandat confié à Firelight :

- Lancer le projet par l'élaboration d'un plan et d'un budget en fonction de l'énoncé des travaux et des objectifs du projet.
- Concevoir les consultations en collaboration avec le Conseil canadien des normes (CCN), notamment en décrivant les méthodes de consultation prévues, en dressant la liste des participants à l'aide d'une méthode adéquate et en préparant des questions et une documentation d'accompagnement.
- Communiquer avec les principaux participants pour planifier les entrevues, gérer la logistique virtuelle et mener les consultations.
- Mener des échanges structurés avec les principales parties prenantes au moyen d'un sondage et d'entrevues individuelles avec les principaux participants.
- Rédiger un rapport sommaire de 15 à 30 pages (le présent rapport) décrivant les consultations et le degré de participation, et présentant en détail les commentaires recueillis.

La version finale du rapport sur les consultations (le présent rapport) devait donner l'essentiel des leçons à retenir et des perspectives autochtones sur la gouvernance des données, et :

- s'appuyer directement sur la recherche, les pratiques exemplaires et le savoir actuellement disponibles en matière de souveraineté des données autochtones;
- présenter si possible les outils et les processus d'enregistrement et de validation des principales données physiques à l'appui des cadres de gouvernance des données autochtones;
- tenir compte des orientations et du savoir recueillis lors des consultations avec les détenteurs du savoir des Premières Nations, des Inuits et des Métis, les spécialistes locaux en gouvernance des données et les organisations autochtones concernées;
- respecter les principes des Premières Nations, des Inuits et des Métis en matière de collecte, de propriété, de conservation et de diffusion des données.

1.3 LIMITES

Le présent rapport est fondé sur les commentaires recueillis pendant un nombre réduit de consultations initiales auprès de groupes autochtones; il est donc sujet à un certain nombre de limites :

- Étant donné les contraintes temporelles et budgétaires, il n'était pas possible d'aborder en détail chacun des 35 enjeux définis par les groupes de travail du CCNGD. Les questions du sondage étaient axées sur les enjeux définis par le groupe de travail 1 (Fondements de la gouvernance des données), alors que les entrevues portaient sur les grands enjeux de gouvernance des données soulevés par les principaux participants.
- Sur les 16 personnes invitées à une entrevue, 8 ont décliné l'invitation pour diverses raisons (manque de temps ou refus de partager ses connaissances avec les chercheurs) ou n'ont pas répondu.
- Bien que le présent rapport soit basé sur la consultation de gouvernements et organisations autochtones, son contenu ne doit pas être interprété comme une représentation de l'ensemble des points de vue autochtones sur les enjeux de gouvernance des données. Comme l'ont souligné des participants tout au long des consultations, les préoccupations, les priorités et les points de vue varient au sein de chaque groupe des Premières Nations, des Inuits et des Métis et d'un groupe à l'autre, tout comme d'une région ou d'un territoire à l'autre au Canada.
- Soulignons tout particulièrement que peu de représentants d'organisations inuites et métisses ont participé aux consultations. Aucune des personnes contactées dans les grandes organisations métisses nationales ou régionales n'ont pu participer aux entrevues, et un seul représentant d'une organisation inuite. *C'est une limite importante du rapport, car il est nécessaire de mieux connaître les perspectives inuites et métisses sur les enjeux de gouvernance des données*.
- Étant donné les contraintes temporelles et budgétaires, la documentation d'accompagnement et le sondage n'ont été diffusés qu'en anglais et en français. Les entrevues ont aussi été menées dans ces deux langues. Des consultations menées dans les langues autochtones permettraient de recueillir davantage d'information, étant donné l'importance de ces langues comme moyen privilégié de transmission de la culture et des façons d'être et d'apprendre.

Compte tenu de ce qui précède, le présent rapport peut être considéré comme un premier compte-rendu des perspectives autochtones sur les enjeux de gouvernance des données et les manières possibles de s'y attaquer. Il faut cependant poursuivre le dialogue afin de cerner et de définir clairement d'autres enjeux, ainsi que pour comprendre comment les perspectives autochtones peuvent contribuer à leur résolution, notamment par l'élaboration éventuelle de normes.

2. Gouvernance des données et communautés autochtones

La souveraineté des données est devenue un sujet important, qui soulève des questions fondamentales sur le droit inhérent d'un organisme souverain de recueillir, contrôler et gérer ses propres données (Snipp, 2016, p. 39). Tout peuple a besoin de données de haute qualité sur sa population, ses communautés, son territoire, ses ressources et sa culture pour prendre des décisions éclairées, et les peuples autochtones ne font pas exception[18]. Pourtant, ces peuples et leurs instances dirigeantes peinent toujours à obtenir leur autonomie en matière de gouvernance des données. À plusieurs égards, les activités de collecte de données sur les peuples autochtones restent des activités de nature politique et logistique assurées par des gouvernements coloniaux. La collecte de données continue ainsi de reproduire et de renforcer des structures coloniales conçues pour gérer les peuples, les terres et les ressources autochtones.

Avec l'accélération et l'élargissement du développement économique, social et culturel des peuples autochtones, les besoins en données augmentent. La prolifération rapide des données a fait émerger la notion de souveraineté des données autochtones, c'est-à-dire le droit d'une instance dirigeante autochtone de diriger la collecte, la propriété, la diffusion et l'application de ses propres données sur ses communautés, ses membres, ses terres et ses ressources. Les peuples sont de plus en plus conscients de l'importance d'affirmer leur souveraineté et de définir des processus de gouvernance exhaustifs pour décoloniser les données. Les Autochtones peuvent maintenant utiliser les données pour répondre à leurs propres besoins et à leurs propres priorités. C'est dans ce contexte que les peuples autochtones remettent en question les discours dominants grâce à des données recueillies par et pour les communautés, reflétant leur vision du monde et respectueuses de leur culture. Lorsqu'elles sont créées, recueillies et utilisées correctement, les données permettent aux peuples autochtones de mettre en lumière des enjeux souvent passés sous silence.

2.1 DÉFIS EN MATIÈRE DE DONNÉES AUTOCHTONES

Nous présentons ici certains des enjeux qui sous-tendent l'ensemble du mouvement en faveur de la souveraineté des données autochtones. Ils révèlent les vestiges incontournables des répercussions sur les peuples autochtones des pratiques non autochtones de collecte et de gestion des données.

2.1.1 Contexte colonial de la collecte et de l'utilisation des données

Le paysage de la souveraineté des données autochtones doit être situé dans le contexte historique et contemporain de la colonisation. Les pratiques actuelles d'élaboration des politiques et de prise de décision sont de plus en plus ancrées dans des projets de collecte de données dirigés par l'État (McMahon et coll., 2017, p. 432).

Dans le passé, les activités de collecte de données sur les populations autochtones étaient surtout menées par des organismes fédéraux et provinciaux, des universités et d'autres acteurs externes, et justifiaient souvent le maintien de structures visant à appliquer des politiques gouvernementales de contrôle, de surveillance et d'assimilation des peuples autochtones. La collecte de données se concrétisait par des indicateurs et des ensembles de données quantitatifs qui reflétaient des préoccupations et valeurs occidentales favorables à l'élimination des économies autochtones, à l'érosion des lois, protocoles et systèmes de connaissances ancestraux, au sapement du leadership autochtone, à la dispersion des Autochtones dans les populations et à l'appropriation des terres et des ressources autochtones (Smith, 2016, p. 117-135). Par exemple, les activités de collecte de données dirigées par l'État infériorisaient les institutions sociales, économiques et politiques autochtones pour justifier et rationaliser l'assimilation violente des peuples dans la société dominante au moyen de structures coloniales comme les pensionnats et la rafle des années 1960 (CVR, 2015). Comme l'ont souligné Raine et coll. (2019, p. 304), les données sur les peuples autochtones véhiculent souvent « une image d'iniquité en privilégiant une vision basée sur des disparités, des privations, des désavantages, des dysfonctions et des différences mesurés statistiquement ».

18 On désigne par « données autochtones » l'ensemble des données, renseignements et connaissances sur les personnes, collectivités, communautés, cultures, savoirs, sciences, cérémonies, terres et ressources autochtones.

Aujourd'hui, la plupart des Autochtones perçoivent toujours la collecte de données comme un moyen de répondre à des intérêts externes plutôt qu'à des besoins et à des priorités autochtones, et comme une façon de discréditer la souveraineté et l'autodétermination autochtones. La nature essentiellement politique de la collecte de données et la persistance des structures coloniales en la matière créent donc un climat de méfiance et expliquent la réticence des Autochtones à communiquer des renseignements (CRPA, 1996).

2.1.2 Extraction des données et exclusion

Étant donné le peu de respect régnant entre les responsables de la collecte de données et les peuples autochtones, les données autochtones ont longtemps été extraites des communautés, ce qui a empêché ces dernières et leurs dirigeants d'affirmer leur autonomie quant aux données les concernant. Notamment, des agents externes – établissements d'enseignement ou organismes gouvernementaux – ont souvent exclu les peuples autochtones de l'interprétation et de la présentation des résultats des recherches basées sur ces données (McBride, 2018, p. 6), et cette exclusion a fréquemment entraîné une interprétation erronée nuisant aux peuples autochtones, voire les infériorisant (McBride, 2018, p.6), comme dans le cas d'une nation Nuu-chah-nulth, en Colombie-Britannique.

Dans ce dossier, un professeur de l'Université de la Colombie-Britannique a recueilli plus de 800 échantillons de sang, à l'origine pour étudier l'incidence accrue de l'arthrite dans la nation Nuu-chah-nulth. Par la suite, sans en informer d'aucune façon la nation, le chercheur a utilisé les échantillons de sang pour produire plus de 200 rapports sur des sujets tout autres – recherche sur le VIH/sida et habitudes migratoires, par exemple – qui ont complètement discrédité les croyances traditionnelles des Nuu-chah-nulth sur la Création (CGIPN, 2016, p. 145).

L'exclusion passée et actuelle des nations autochtones les privant de toute autonomie sur les données les concernant a contribué à perpétuer leur méfiance quant à la collecte de données en général. Comme le montre le dossier des Nuu-chah-nulth, les données sont souvent utilisées au mépris de la volonté des nations autochtones et des ententes conclues avant le début des recherches (Raine et coll., 2017, p. 4). Steffler (2016, p. 151) rappelle d'ailleurs que « cette approche a miné la confiance, l'adhésion et la participation des communautés autochtones, ce qui n'a pas manqué de nuire à la qualité globale des données ». Par conséquent, les pratiques universitaires occidentales de collecte de données ont toujours des effets résiduels qui entretiennent le climat de méfiance et de suspicion, et la réticence à l'échange d'information entre les peuples autochtones et les acteurs externes.

2.1.3 La recherche ne reflète ni les besoins ni les priorités des Autochtones

Dans le passé, la collecte, la gestion et la diffusion de données autochtones se sont faites sans la participation ou le consentement éclairé des Autochtones. Par conséquent, la plupart des données recueillies sur leurs peuples sont inexactes, manquent de pertinence et correspondent à un point de vue colonial. Comme le souligne le *Rapport de la Commission royale sur les peuples autochtones* (CRPA, 1996), les données sur les peuples autochtones sont toujours vues comme servant des intérêts extérieurs, largement en raison des répercussions complexes du colonialisme, qui perdurent[19].

19 « La collecte d'informations et leur utilisation ultérieure sont essentiellement de nature politique. Dans le passé, on ne demandait pas aux autochtones quelles informations il fallait recueillir, qui devrait s'en charger, qui devrait le tenir à jour, ni qui devait y avoir accès. Ces informations ne correspondaient pas nécessairement aux questions que se posaient les peuples autochtones, à leurs priorités et à leurs préoccupations. Comme la collecte de données a fréquemment été imposée de l'extérieur, elle s'est fréquemment heurtée à des résistances. (CRPA, 1996) »

Il importe de souligner que les peuples autochtones ont été étudiés à l'extrême, constamment ciblés par une collecte de données dirigée par l'État qui profite principalement à des entités externes comme les gouvernements, les entreprises ou les établissements de recherche. L'imposition de pratiques de collecte de données occidentales prive les peuples autochtones d'une participation authentique : les entités externes présentent « à une communauté des concepts de recherche déjà préparés, souvent déjà financés, plutôt que de lui proposer une collaboration dès le départ » (CGIPN, 2016, p. 143). Souvent, de telles initiatives empêchent une participation authentique et un consentement éclairé des Autochtones, et les données recueillies sont susceptibles d'être surexploitées et mal interprétées. Par conséquent, les activités de collecte de données échouent à refléter les aspirations et besoins autochtones.

De nombreux processus de collecte de données dirigés par l'État sont lancés par les administrations fédérales et provinciales qui définissent les paramètres de recherche et de mesure. La majorité des recherches menées sur les peuples autochtones infériorisent les communautés autochtones, se concentrant sur les problèmes de santé chroniques comme le diabète, l'alcoolisme et le suicide (CGIPN, 2014). Si ces études sont importantes, elles réduisent les expériences vécues par les Autochtones à des données statistiques, et échouent à traiter des conséquences de la colonisation, comme les traumatismes intergénérationnels, le racisme systémique et la violence fondée sur le genre (CGIPN, 2014; Dewar, 2019, p.4).

2.2 GOUVERNANCE ET SOUVERAINETÉ DES DONNÉES AUTOCHTONES : PROPRIÉTÉ, CONTRÔLE ET REPRÉSENTATION

2.2.1 Souveraineté des données autochtones

La souveraineté des données est un concept propre au 21e siècle, étroitement lié à l'évolution rapide de la création, de la transformation et de l'accessibilité des données. Le concept renvoie au fait que les données sont assujetties aux lois et aux structures de gouvernance de l'endroit où elles se trouvent.

Le concept de souveraineté des données autochtones a émergé en réaction au rôle passé et actuel de la production de connaissances dans la perpétuation de relations coloniales entre les gouvernements et organisations autochtones et le gouvernement du Canada (Espey, 2002). C'est un concept qui donne lieu à tout un éventail de considérations légales, éthiques et pratiques. La souveraineté des données autochtones affirme le droit des peuples autochtones de diriger la collecte, la diffusion, la propriété et l'administration de leurs propres données (Kukutai et Taylor, 2016), droit qui découle du droit d'une entité souveraine de gouverner sa population, ses terres et ses ressources. La tendance à décoloniser les données fait émerger des pratiques de souveraineté des données autochtones, ce qui se traduit par toute une gamme de modèles de gouvernance.

La souveraineté des données autochtones se base sur les principes suivants :

1. Les données d'une instance dirigeante autochtone comprennent tous les faits, connaissances et renseignements sur son peuple, ses communautés, ses terres et ses ressources.
2. Les activités de recherche et de collecte de données reflètent les besoins et les priorités d'une nation autochtone.
3. Les peuples autochtones sont authentiquement mobilisés et consultés pour tous les aspects du processus de recherche.
4. La recherche adopte des processus respectueux de la culture autochtone, qui reflètent les visions du monde, les valeurs, l'éthique et les protocoles autochtones.
5. Les instances dirigeantes autochtones ont pleins pouvoirs sur la collecte, la propriété et l'application des données.
6. Les données restent assujetties aux lois et protocoles traditionnels d'une communauté autochtone.

Des processus de collecte, d'analyse et de gérance des données conçus par et pour les peuples autochtones constituent un atout précieux pour leur autonomie, leur développement et leurs aspirations. En d'autres mots, les données autochtones représentent un aspect important de la souveraineté autochtone dans son ensemble, et du mouvement vers l'autonomie gouvernementale, l'autodétermination et la décolonisation.

2.2.2 Gouvernance des données autochtones

Le concept de souveraineté des données autochtones est lié à celui de la gouvernance de ces données, qui prévoit les mécanismes d'application du droit inhérent des peuples autochtones au contrôle de la collecte, de la diffusion, de l'administration et de l'application de leurs propres données. Les peuples autochtones, dont les systèmes de connaissances traditionnels ont souvent été perturbés et assimilés par les pratiques coloniales occidentales, réaffirment leur autonomie par des mécanismes de gouvernance des données autochtones (Lovett et coll., 2019).

La gouvernance des données autochtones se base sur les principes suivants :

1. Les instances dirigeantes autochtones obtiennent le pouvoir décisionnel d'affecter les tâches et responsabilités relatives à l'administration de toutes les données les concernant.
2. Les instances dirigeantes autochtones obtiennent le pouvoir décisionnel relatif à la conception, l'interprétation, la validation, la propriété, l'accessibilité et l'utilisation de toutes les données les concernant.
3. Les instances dirigeantes autochtones obtiennent le pouvoir décisionnel d'établir leurs propres mesures et définitions culturellement appropriées à utiliser dans les processus de production, de propriété, d'analyse et d'administration des données.

La gouvernance des données autochtones est le cadre directeur qui permet la souveraineté des données autochtones. La section 4 donne des exemples d'importantes initiatives de gouvernance des données autochtones; ces initiatives prévoient les mécanismes nécessaires à un groupe pour atteindre la souveraineté des données par l'affirmation de la propriété, du contrôle et de la représentation dans la collecte, la diffusion et l'administration de ses propres données.

3. Méthodes

La consultation consistait en un sondage en ligne et des entrevues avec les principaux participants. Les méthodes employées dans les deux cas sont décrites ci-dessous, y compris pour le choix des participants, l'enregistrement du consentement éclairé et l'analyse.

3.1 CONSENTEMENT ÉCLAIRÉ ET ADMINISTRATION DES DONNÉES RECUEILLIES

Tous les participants ont fourni un consentement éclairé avant de participer au sondage ou aux entrevues. Dans les deux cas, le formulaire de consentement éclairé décrivait les objectifs et les processus de la consultation de même que le contexte global de l'élaboration de la feuille de route du CCNGD, les données recueillies et la façon de les administrer. Le formulaire de consentement de l'entrevue se trouve à l'annexe 1, et le texte du sondage (incluant le formulaire de consentement) est à l'annexe 2.

3.1.1 Sondage

Un formulaire de consentement d'une page a été ajouté au sondage, immédiatement après la page de présentation. Après avoir pris connaissance des travaux et de la façon dont l'information serait recueillie et administrée, le participant devait indiquer s'il donnait son consentement. S'il refusait, le sondage s'arrêtait sans recueillir aucune donnée autre que son refus. S'il acceptait, il était dirigé vers la première question du sondage. Le participant trouvait sur la page de consentement les coordonnées de l'équipe de Firelight, à qui il pouvait s'adresser pour poser des questions sur le processus de consultation. La participation au sondage était anonyme et les réponses, confidentielles. Les répondants ne devaient donner aucune information permettant de les identifier. Pour encourager la participation, on leur donnait la chance de gagner une carte-cadeau de 100 $ (en répondant à un questionnaire séparé à partir d'un hyperlien donné à la dernière page du sondage).

Les données recueillies ont été enregistrées sur les serveurs de SurveyMonkey jusqu'à la fin du sondage, le 2 février 2021. Elles ont ensuite été transférées sur un serveur sécurisé situé au Canada, propriété du Groupe Firelight, où elles se trouvent toujours. Toutes les données seront détruites dans l'année suivant leur collecte.

3.1.2 Entrevues avec les principaux participants

Au début de chaque entrevue, le formulaire de consentement (voir l'annexe 1[20]) était passé en revue avec chacun des participants. Sur ce formulaire, après une description de l'objectif de l'entrevue et du mode d'utilisation et de conservation des renseignements recueillis, figuraient des questions aux participants quant à leur participation à l'entrevue.

Le formulaire de consentement précisait que les principaux participants resteraient propriétaires de leurs réponses. Après chaque entrevue, chacun des participants en a reçu la transcription et l'enregistrement, et conservait les droits associés. Les enregistrements des entrevues sur Zoom ont d'abord été sauvegardés localement sur un ordinateur portable, puis transférés sur un serveur sécurisé situé au Canada et appartenant au Groupe Firelight. Des copies des entrevues et des données seront stockées sur ce serveur jusqu'à leur destruction, au plus tard un an après leur collecte.

Sur le formulaire de consentement, les participants devaient également indiquer s'ils acceptaient d'être cités, comment ils souhaitaient être nommés dans l'affirmative, et s'ils désiraient que leur nom soit mentionné dans le rapport. Les participants conservaient le droit de retirer leur consentement pour toutes ces questions. Chaque participant a reçu la version préliminaire du rapport et avait la possibilité de modifier les interprétations et les citations avant la production de la version finale. Les principaux participants ont reçu un numéro d'identification personnel (NIP) prenant la forme I## pour assurer la confidentialité. Pour désigner les participants qui avaient choisi de ne pas voir leur nom associé aux citations, nous avons utilisé le NIP; ainsi, les auteurs des citations sont tour à tour désignés par leur nom et par un NIP tout au long du rapport. Les citations et leur attribution ne sont donc utilisées dans le présent rapport qu'avec la permission des personnes concernées, tout comme les noms n'y sont mentionnés qu'avec leur autorisation.

Le consentement aux entrevues pouvait prendre deux formes. Après avoir lu et étudié le formulaire de consentement avec le représentant de Firelight, chaque participant donnait verbalement son consentement au début de chaque enregistrement. Chaque participant signait également une copie imprimée du formulaire avant de la renvoyer à Firelight. Comme les entrevues étaient menées à distance et que certains n'avaient pas accès à une imprimante et à un scanneur pour signer et renvoyer une copie imprimée du formulaire de consentement, le consentement pouvait être uniquement verbal.

3.2 SONDAGE

Dans une première étape, la consultation a pris la forme d'un sondage en ligne pour joindre le plus de monde possible dans les délais prévus. Le sondage visait à nous permettre de comprendre : les enjeux de gouvernance des données les plus importants pour les groupes autochtones, les initiatives ou normes permettant de traiter ces enjeux, et le point de vue des répondants quant à l'avenir de la gouvernance des données autochtones. Une plate-forme en ligne a été choisie comme le meilleur moyen de joindre le maximum de répondants pendant la pandémie.

20 Certains participants ont demandé qu'on précise dans le formulaire de consentement la nature, la propriété et le mode d'utilisation et de conservation des données recueillies, ainsi que le fait que le participant conservait le droit de retirer son consentement à l'inclusion de ses données dans le rapport. Le formulaire de consentement fourni à l'annexe 1 constitue la version la plus exhaustive et détaillée de la description du mode de collecte, de propriété et de conservation des données dans le cadre de cette consultation.

À l'origine, la consultation visait à recueillir des commentaires sur les 35 enjeux définis par les quatre groupes de travail du CCNGD. Lors des rencontres de préparation et de conception de la consultation, Firelight et le CCN se sont cependant rendu compte que les contraintes temporelles et budgétaires ne permettraient pas de couvrir tous ces enjeux en profondeur. Ils ont aussi déterminé qu'un sondage cherchant à recueillir des commentaires sur les 35 enjeux serait trop lourd et obtiendrait un taux de participation moins grand. Pour cette raison, les questions du sondage se concentrent sur les enjeux définis par le groupe de travail 1 (Fondements de la gouvernance des données) :

- Cadre des responsabilités
- Attestations encadrant les rôles professionnels
- Habileté numérique
- Cybersécurité et protection des données
- Gouvernance de la gestion des données
- Protection des renseignements personnels
- Directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique
- Données ouvertes et procédures d'harmonisation et d'interopérabilité des données
- Rôle des acteurs et des opérations de traitement des données
- Réutilisation des données

Nous avons choisi une méthode mixte utilisant à la fois des questions ouvertes et fermées afin d'obtenir des données quantitatives et qualitatives. Le sondage en ligne a été conçu et réalisé sur la plate-forme SurveyMonkey. Il existe deux versions du sondage, une en anglais et l'autre en français.

Nous avons joint les répondants de plusieurs façons : partage des liens menant aux deux versions du sondage sur les médias sociaux de Firelight et du CCN en anglais et en français (Facebook, Twitter, Instagram et LinkedIn) et par courriel aux membres des réseaux de Firelight. Au total, les liens ont été communiqués publiquement dans les réseaux de Firelight par 18 messages sur les plates-formes de médias sociaux du 12 au 26 janvier 2021. Ils ont aussi été diffusés sur une plate-forme Mighty Networks du Indigenous Mapping Collective, qui regroupe de plus de 650 praticiens de la cartographie autochtone au Canada et à l'étranger. Le personnel de Firelight a également communiqué les liens dans ses réseaux par courriel. Le matériel promotionnel est présenté ici à l'annexe 4.

Les résultats du sondage (données quantitatives et qualitatives) figurent à la section 4. La section 4.1 donne également un aperçu des résultats de la consultation à diffuser dans les réseaux de Firelight.

3.3 ENTREVUES AVEC LES PRINCIPAUX PARTICIPANTS

Nous avons mené des entrevues auprès de praticiens et d'experts de la gouvernance des données autochtones afin de bien comprendre les points de vue autochtones sur les enjeux de gouvernance des données. À ce jour, les groupes de travail du CCNGD ne comptent aucun représentant autochtone : cela signifie que la définition des enjeux de gouvernance des données ne tient pas compte des points de vue autochtones. Les entrevues, axées sur les grands enjeux de la gouvernance des données soumis par les principaux participants, visaient à permettre aux experts de la gouvernance des données autochtones de lancer le processus de définition et de cadrage des enjeux de manière jugée appropriée et pertinente pour leur travail. Pour que les participants puissent souligner les enjeux et initiatives les plus importants pour eux, les questions d'entrevue étaient générales (voir le guide d'entrevue à l'annexe 3) et l'entrevue était semi-structurée.

Les principaux participants ont été choisis en fonction de leur expertise et de leur expérience de travail dans des organisations, des projets ou des initiatives axés sur la gouvernance des données autochtones. Firelight s'est efforcée de communiquer avec des experts des différents contextes des communautés des Premières Nations, des Inuits et des Métis, tout en faisant de la diversité des régions et des disciplines une priorité. Dans le même esprit, elle a passé en revue les initiatives sur la gouvernance et la souveraineté des données autochtones au Canada, de même que la littérature pertinente. Elle a ainsi dressé une liste de communautés, de réseaux et d'organisations, parmi lesquels elle a isolé ceux qui travaillent particulièrement sur la gouvernance et la souveraineté des données autochtones comme potentiels principaux participants. Elle a également obtenu des recommandations à cet égard de la part du personnel du CCN et lors d'entrevues avec certains des principaux participants.

Au total, 16 personnes ont été contactées par téléphone ou par courriel du 18 janvier au 18 février 2021, et invitées à une entrevue. Parmi elles, huit travaillaient dans des organisations de Premières Nations, deux dans des organisations nationales inuites, cinq dans des organisations ou initiatives métisses, et une dans une organisation traitant des données des Premières Nations, des Inuits et des Métis. Au total, huit invités ont accepté de participer à une entrevue, cinq ont décliné l'invitation, et trois n'ont répondu ni à l'invitation ni aux rappels.

Aucun des représentants d'organisations métisses nationales ou régionales n'a été en mesure de participer aux entrevues ou de répondre à l'invitation. L'un d'entre eux a donné le nom d'un collègue qui pourrait répondre à sa place. Le manque de temps faisait partie des raisons invoquées pour décliner l'invitation; par ailleurs, l'un des invités a refusé de communiquer ses connaissances aux chercheurs. Un autre a expliqué que son organisation aurait eu besoin de plus de temps pour préparer une telle entrevue. L'une des personnes qui ont décliné l'invitation a expliqué qu'il faudrait une consultation plus approfondie qu'une entrevue et un sondage pour saisir le point de vue autochtone sur les enjeux de gouvernance des données dans toute sa complexité.

Deux invités ont demandé à être accompagnés de collègues lors de l'entrevue; au total, douze personnes ont donc participé aux huit entrevues. Dix d'entre elles œuvraient au sein d'organisations des Premières Nations, une dans une organisation inuite, et une dans une organisation qui s'occupe de gouvernance des données des Premières Nations, des Inuits et des Métis. Le tableau 1 présente la liste des participants. Comme ceux-ci pouvaient choisir la façon dont ils seraient nommés dans le tableau 1, certains noms n'y figurent pas.

Tableau 1 : Principaux participants

Mindy Denny, Union of Nova Scotia Mi'kmaq
Chercheur ou chercheuse autochtone, Université de Guelph
Samantha Michaels, conseillère principale en politiques, Pauktuutit Inuit Women of Canada
Membre du personnel de la Commission de la santé et de services sociaux des Premières Nations du Québec et du Labrador (CSSSPNQL)
Gwen Phillips, nation Ktunaxa, championne de l'Initiative de gouvernance des données en Colombie-Britannique
Jullian MacLean, Hotìı ts'eeda (unité de soutien de la SRAP des T.N.-O)
Aaron Franks, conseiller principal, Centre de gouvernance de l'information des Premières Nations
Nancy Gros-Louis McHugh, gestionnaire du secteur de la recherche, Commission de la santé et de services sociaux des Premières Nations du Québec et du Labrador (CSSSPNQL)
Erin Corston, conseillère principale, Centre de gouvernance de l'information des Premières Nations
Patrice Lacasse, conseiller en gouvernance, Commission de la santé et de services sociaux des Premières Nations du Québec et du Labrador (CSSSPNQL)
Membre du personnel, Conseil des Premières nations du Yukon

Les entrevues ont été menées à distance à l'aide du logiciel de vidéoconférence Zoom par deux employés de Firelight (l'un posait les questions et l'autre prenait des notes). Les enregistrements audio et vidéo des entrevues (d'une durée de 30 à 70 minutes) ont été sauvegardés localement sur les ordinateurs portables des chercheurs de Firelight. Sept entrevues ont été menées en anglais et une huitième principalement en français. Chaque entrevue a ensuite été transcrite, puis analysée. Chaque participant a reçu un NIP (I##) pour préserver la confidentialité.

3.4 ANALYSE

Nous avons analysé les transcriptions des entrevues et les données qualitatives tirées des réponses aux questions ouvertes du sondage pour en dégager les grands thèmes, dont certains concernaient des enjeux particulièrement importants pour les principaux participants et d'autres portaient sur les solutions possibles aux problèmes de gouvernance des données et sur l'avenir de la gouvernance des données autochtones. Enfin, nous avons ajouté à ces thèmes les dix enjeux définis par le groupe de travail 1 du CCNGD dans des tableaux servant à coder les données quantitatives, afin de faire émerger les liens entre ces enjeux et ceux soulevés par les participants. Nous avons ajouté à ces tableaux une couche supplémentaire d'information, soit la région où travaille le participant, de même que l'appartenance de son organisation – Premières Nations, Inuits ou Métis – pour mieux cerner les particularités des enjeux dans différents contextes régionaux et culturels.

4. Résultats

Nous présentons ici les résultats de la consultation : la section 4.1 fait état des résultats du sondage en ligne, les sections 4.2 et 4.3 décrivent les principaux enjeux de même que les initiatives qui existent déjà pour y répondre, et la section 4.4 résume les commentaires des participants sur l'avenir de la gouvernance des données autochtones.

4.1 SONDAGE

4.1.1 Promotion

Au total, les annonces du sondage sur les plates-formes des médias sociaux ont été vues par 6 687 utilisateurs, dont 224 ont réagi (par un commentaire, un partage, un clic ou une mention « j'aime »). Cela comprend 123 clics sur le lien menant au sondage en ligne. Les annonces sur les médias sociaux ont été partagées au total 22 fois sur Facebook, Twitter, et LinkedIn. Le tableau 2 résume le nombre total d'utilisateurs joints sur chaque plate-forme de même que le nombre de réactions.

Tableau 2 : Résumé des réactions aux annonces sur les médias sociaux

Plate-forme	Langue	Nombres d'utilisateurs touchés	Nombre de réactions (commentaire, partage, clic ou mention « j'aime »)	Nombre de clics
Facebook	Anglais, français et bilingue	582	20	11
Twitter	Anglais et français	4 086	83	61
LinkedIn	Anglais, français et bilingue	1 369	92	51
Instagram	Anglais, français et bilingue	Inconnu	25	Inconnu
Indigenous Mapping Collective	Anglais	Plus de 650	4	Inconnu
Total		**6 687**	**224**	**123**

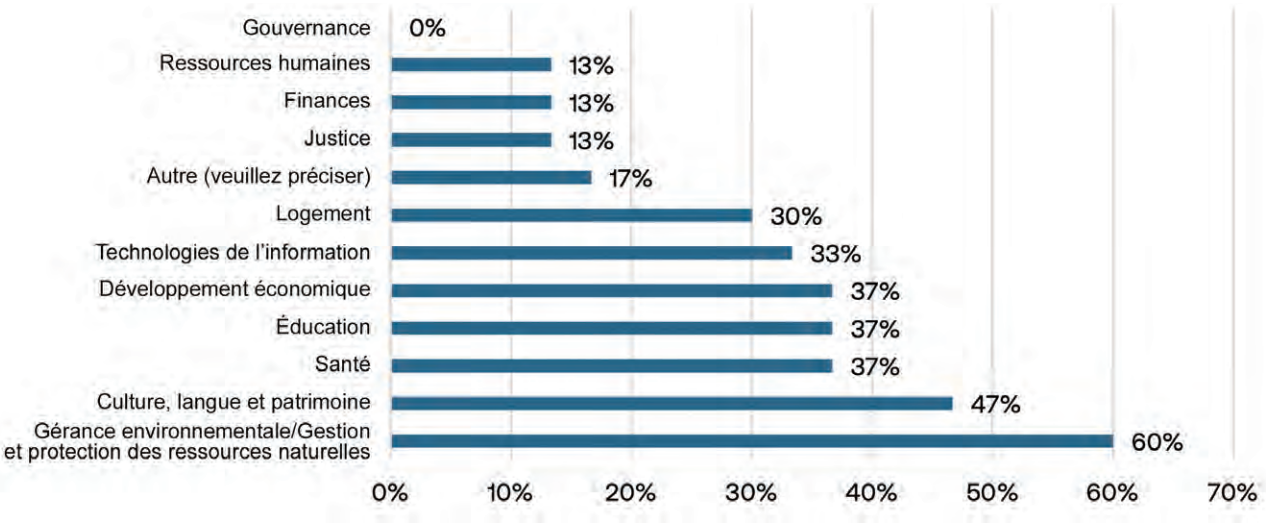
4.1.2 Participation

Le sondage s'est déroulé du 12 janvier au 2 février 2021. Nous avons enregistré 37 répondants à la version anglaise, dont 36 ont donné leur consentement (un refus). Personne n'a répondu à la version française.

Comme les problèmes de gouvernance des données diffèrent d'une population autochtone à l'autre, nous souhaitions nous assurer que la recherche couvrait un éventail de points de vue; nous avons donc demandé aux participants auprès de quelle population autochtone ils travaillaient. Sur les 30 personnes qui ont répondu à cette question, 29 ont dit traiter des données des Premières Nations, 6 des données des Inuits et 6 des données des Métis.

Les répondants ont dit traiter toutes sortes de données (voir la figure 1) : ressources humaines; technologies de l'information; culture, langue et patrimoine; et gestion des ressources naturelles. Les types de données les plus souvent mentionnés étaient la gérance environnementale de même que la culture, la langue et le patrimoine.

Figure 1 : Types de données autochtones traitées par les participants

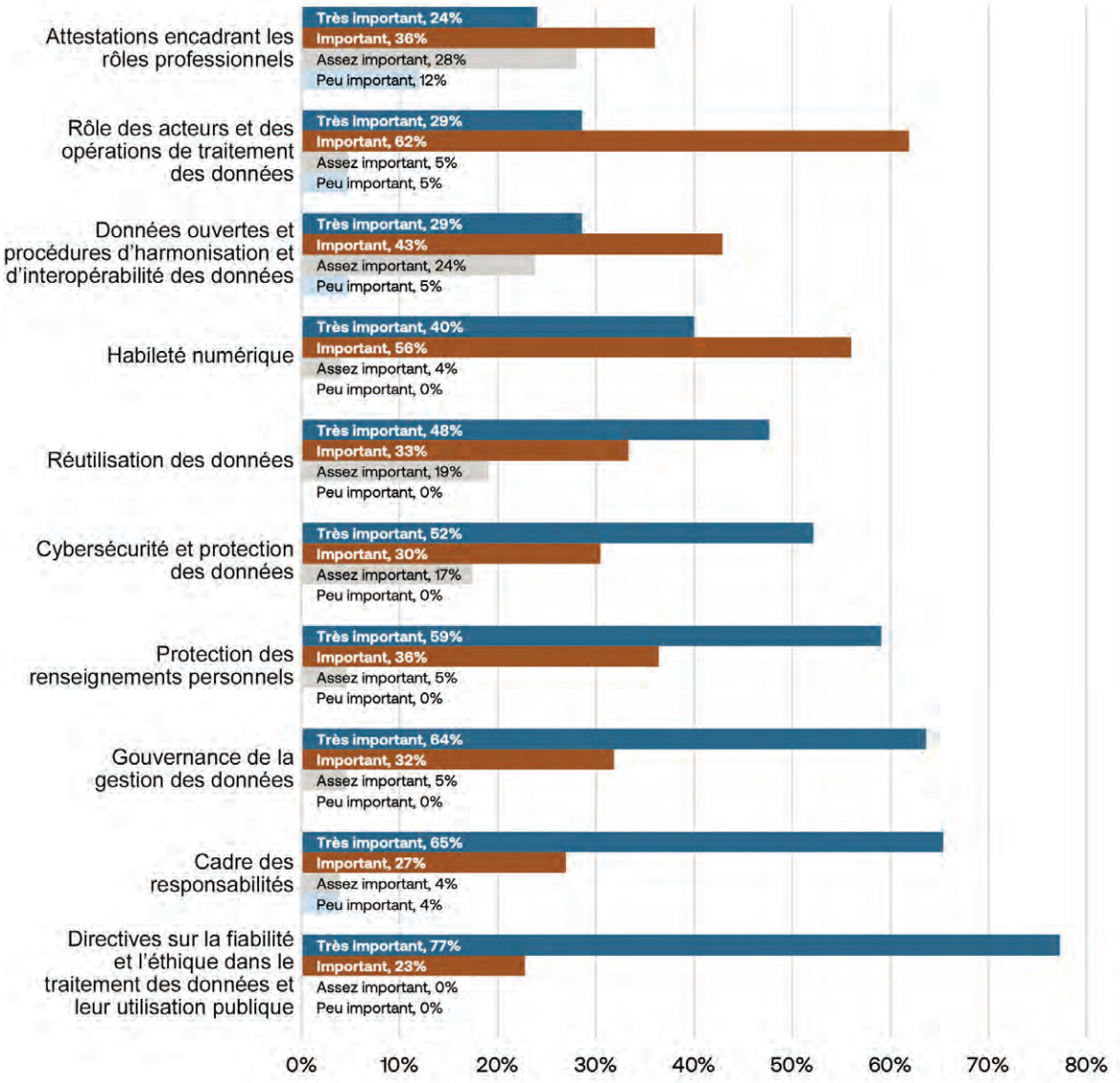


4.1.3 Classement des enjeux

Après avoir présenté aux participants les dix principaux enjeux soulignés par le groupe de travail 1 du CCNGD, nous leur demandions de les classer en fonction de leur importance pour la gouvernance des données autochtones, sur une échelle à cinq niveaux (de *pas important* à *très important*, le niveau du milieu étant *assez important*). Les participants n'avaient pas à comparer les enjeux entre eux, mais simplement à les coter individuellement. Chacune des questions de classement était suivie d'une question ouverte leur permettant d'expliquer leur point de vue sur cet enjeu. Les résultats du classement sont présentés à la figure 2.

Les directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique et le cadre des responsabilités sont les enjeux les plus fréquemment jugés *très importants* par les participants pour l'élaboration de normes sur la gouvernance des données. Parmi eux, 62 % ont convenu que la définition du rôle des acteurs et des opérations de traitement des données était un enjeu *important*; c'est d'ailleurs l'enjeu le plus fréquemment jugé important, suivi de l'habileté numérique avec 56 %. Aucun des enjeux n'a été jugé sans importance.

Figure 2 : Importance accordée par les participants au sondage aux dix enjeux des fondements de la gouvernance des données cernés par le groupe de travail 1 du CCNGD



4.1.4 Commentaires sur les principaux enjeux

À partir des réponses aux questions ouvertes sur les dix principaux enjeux, une série de thèmes se dégagent, dont l'un des principaux est la nécessité de restaurer la confiance dans les relations avec les groupes autochtones. Les participants ont souligné que la confiance devait faire partie intégrante des normes sur le cycle de vie et la conservation des données, et se trouvait au cœur de l'avancement de la gouvernance et de la souveraineté des données autochtones.

Un second thème concerne la nécessité de confier aux Autochtones la direction et l'administration des programmes de collecte des données dans leurs communautés, sur leurs territoires et pour eux-mêmes. Un participant a notamment souligné que la collecte de données devait être dirigée par les Autochtones et leurs communautés plutôt que par des parties et des systèmes externes.

Tout en remettant en contexte le principal enjeu – Directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique –, l'un des participants a souligné qu'il était vraiment important de créer des comités d'éthique et d'examen dirigés par des Autochtones pour approuver, superviser et interpréter les normes de gouvernance des données autochtones. Le tableau 3 résume d'autres thèmes mis en lumière par les réponses des participants sur les dix principaux enjeux de gouvernance des données.

Tableau 3 : Commentaires des participants sur les principaux enjeux cernés par le groupe de travail 1

Enjeu	Réponses qualitatives
Cadre des responsabilités	Les principaux thèmes liés à cet enjeu sont la définition des concepts et des rôles en gouvernance des données autochtones, l'élaboration de méthodes culturellement appropriées à cet égard et l'utilisation de principes bien établis comme les principes de PCAP® dans la création de normes de gouvernance des données autochtones. Voici des commentaires des participants : Il importe de définir et de distinguer *responsabilité* et *reddition de comptes*. Par ailleurs, les normes doivent garantir que les établissements et les chercheurs rendent des comptes aux groupes autochtones avec qui ils travaillent. La *Loi sur la protection des renseignements personnels* est une bonne ressource pour l'élaboration de normes sur cette question. De plus, certains gouvernements et organisations autochtones ont conclu des ententes de partage des données pour la gestion des connaissances traditionnelles, ententes qui peuvent aussi servir de référence. Certains types de données (par exemple les données d'arpentage) sont régis par des systèmes étrangers. Il peut alors être difficile pour un groupe ou une organisation autochtone de savoir à qui demander des comptes. Les normes doivent traiter de cette question. Il faut s'assurer que les principes de PCAP® des Premières Nations sont vraiment appliqués et que les organisations ne s'en servent pas simplement comme façade.
Attestations encadrant les rôles professionnels	Les principaux thèmes liés à cet enjeu sont le développement des compétences (la formation) et la souveraineté des données autochtones. Voici des commentaires des participants : La certification et la formation devraient inclure l'amélioration de la compétence culturelle des professionnels travaillant avec les groupes autochtones. Les normes portant sur cet enjeu devraient inclure des politiques sur la surveillance et la supervision pour assurer un certain professionnalisme et le maintien de la certification des professionnels. Les personnes responsables des données autochtones (les administrateurs) devraient suivre une formation officielle sur la protection des renseignements personnels. Ou alors, une personne de l'organisation devrait suivre cette formation et être responsable de cette question. Les obstacles systématiques qui empêchent indûment les Autochtones de recueillir des données, d'en superviser le traitement et de les utiliser pour prendre des décisions les concernant, eux et leur bien-être, doivent être abolis.

Habileté numérique	Le principal thème lié à cet enjeu est la compétence (la formation). Voici des commentaires des participants : Il faut améliorer l'habileté numérique des populations autochtones. Il ne s'agit pas seulement d'utiliser des programmes informatiques, mais également d'avoir les habiletés et connaissances nécessaires pour comprendre ce qui advient des données après leur collecte et comment elles sont traitées.
Cybersécurité et protection des données	Les principaux thèmes liés à cet enjeu sont le financement et le développement des compétences (la formation). Voici des commentaires des participants : Il est parfois coûteux de tenir à jour les systèmes de cybersécurité. Cependant, la qualité de ces systèmes ne doit pas être négligée. Les normes doivent garantir que des systèmes de haute qualité sont en place et fonctionnels. Les groupes autochtones ont besoin de formation pour mettre en place et évaluer leurs propres systèmes et pour surveiller leurs interactions avec les autres systèmes.
Gouvernance de la gestion des données	Les principaux thèmes liés à cet enjeu sont le développement des compétences (la technologie et la formation) et la confiance. Voici des commentaires des participants : Les communautés autochtones doivent être mieux formées pour que les initiatives autochtones de gestion et de gouvernance des données préservent la souveraineté des données autochtones à l'échelle locale, régionale et nationale. Historiquement, l'utilisation des données recueillies sur les groupes autochtones n'a pas toujours donné lieu à des répercussions positives pour ces groupes. Ces derniers doivent participer à tous les aspects de l'élaboration des normes de gouvernance des données autochtones afin d'inspirer confiance aux citoyens et de leur rendre des comptes, et idéalement d'entraîner une plus grande adhésion et une hausse de la qualité et de la quantité des données recueillies.
Protection des renseignements personnels	Les principaux thèmes liés à cet enjeu sont la confiance, les compétences (la technologie et la formation) et l'élaboration de normes culturellement appropriées. Ces trois thèmes sont étroitement liés et tournent autour de l'idée que l'élaboration de normes sur la confidentialité des données autochtones doit être dirigée par des gouvernements et organisations autochtones. Cependant, ces derniers doivent comprendre les enjeux. De plus, une fois les normes élaborées, il faudra des agents autochtones de protection des renseignements personnels pour en surveiller l'application. Un participant a souligné que les principes de PCAP® des Premières Nations devraient servir à encadrer ce processus. Un autre a fait remarquer qu'il fallait mieux comprendre l'influence des lois provinciales et fédérales sur la protection des renseignements personnels sur le consentement préalable libre et éclairé à l'échelle communautaire, régionale et nationale.
Directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique	Les principaux thèmes liés à cet enjeu sont la confiance, la compétence, l'éthique, la souveraineté des données autochtones et la supervision. Voici des commentaires des participants : Les principes de PCAP® des Premières Nations, tels que définis par les détenteurs de droits des Premières Nations, devraient encadrer l'élaboration de normes sur cet enjeu dans le contexte des données des Premières Nations. Un participant a souligné qu'il fallait mieux soutenir les comités d'éthique et d'examen régionaux des Premières Nations pour leur permettre d'affirmer leur propre souveraineté sur les données afin que celles-ci ne soient pas utilisées sans leur approbation, leur supervision et leur interprétation. Un participant a également souligné qu'il fallait simultanément « se pencher sur le passé, le présent et l'avenir ». Il subsiste de nombreux traumatismes dans les communautés; il faut les guérir pour bâtir la confiance et des relations saines entre tous les acteurs du cycle de vie des données autochtones.
Données ouvertes et procédures d'harmonisation et d'interopérabilité des données	Les principaux thèmes liés à cet enjeu sont les normes culturellement appropriées et les compétences. Voici des commentaires des participants : S'il est important pour les groupes autochtones de partager les données, ce partage ne doit pas se faire au détriment des Autochtones. Dans cet esprit, on souligne que les normes doivent être encadrées par des processus régionaux lancés et appuyés par des protocoles et pratiques autochtones pour garantir le caractère inclusif de l'accès aux données, de la production de rapports et de l'interprétation.

Rôle des acteurs et des opérations en matière de traitement des données	Les principaux thèmes liés à cet enjeu sont le développement des compétences (la technologie et la formation), une définition claire des rôles, et l'élaboration de normes culturellement appropriées. Voici des commentaires des participants : Le personnel des organisations autochtones devrait être formé pour pouvoir exécuter correctement ses tâches de gestion des données, à l'interne comme à l'externe. Il doit aussi avoir accès aux ressources nécessaires pour exécuter ces tâches. Les rôles doivent être clairement définis, consignés et convenus. Cela peut réduire les chevauchements et combler les lacunes. En plus d'avoir les compétences nécessaires à un travail, les acteurs du traitement des données autochtones doivent être encadrés par des normes basées sur des principes éthiques solides, axés sur les valeurs autochtones.
Réutilisation des données	Les principaux thèmes liés à cet enjeu sont le consentement, l'éthique et le respect de considérations éthiques régionales. Voici des commentaires des participants : Actuellement, la collecte, le traitement, l'interprétation et la revente des données autochtones semblent constituer un marché largement déréglementé. Cela doit changer. Les transferts de données devraient comprendre un consentement standard garantissant le maintien de la valeur des données, la protection des participants et le respect. Le consentement devrait expliquer clairement qui aura accès aux données et comment, et combien de temps les données seront conservées, entre autres. Le consentement devrait être communiqué de façon culturellement appropriée, de façon à ce que les participants autochtones comprennent ce qu'ils acceptent. Il faudrait que des organismes de supervision régionaux participent pleinement à l'élaboration de normes de consentement.

Nous avons demandé aux participants s'ils avaient des préoccupations relatives à la gouvernance des données autochtones qui n'étaient pas couvertes par la liste des dix enjeux. Ils nous ont entre autres parlé de la gouvernance des données relatives aux photographies, aux chants, aux médias sociaux, aux entrevues et à d'autres données partagées en ligne ou lors d'interactions quotidiennes, faisant remarquer qu'il fallait des normes pour garantir que des métadonnées soient transmises en même temps que les ensembles de données principaux afin de permettre le suivi et le maintien de la propriété et des droits autochtones sur ces données. Les participants ont également noté qu'il fallait des normes pour faciliter une approche échelonnée du consentement, de la confidentialité et des autorisations. Une telle approche permet d'accorder un niveau d'autorisation différent lors du partage de données et de connaissances selon qu'il s'agit de membres de la famille, d'organisations régionales, de gouvernements, d'industries ou d'autres entités.

4.2 PRINCIPAUX ENJEUX

Cette section présente les principaux enjeux soulevés pendant les entrevues et dans les réponses aux questions ouvertes du sondage. Elle est principalement basée sur les données qualitatives recueillies pendant les entrevues avec les principaux participants, à partir des enjeux soulevés dans les réponses au sondage. Là où c'est pertinent, des citations directes tirées des entrevues illustrent les commentaires recueillis.

4.2.1 Reconnaissance de l'autorité

Je dirais que le principal obstacle à la gouvernance des données par les Premières Nations est la persistance de la non-reconnaissance de ces nations en tant que gouvernements souverains. (I01)

Des participants ont souligné que le plus grand obstacle pour les groupes autochtones en matière de gouvernance des données résidait dans la non-reconnaissance des gouvernements autochtones en tant que décideurs souverains quant à tous les aspects du cycle de vie des données relatives à leur population et à leurs territoires. Pour les participants, c'est la source des autres enjeux rapportés ici. L'un d'entre eux a souligné que même si certains documents gouvernementaux reconnaissent ce rôle des Premières Nations, cela n'a pas pour autant permis à ces dernières d'exprimer activement et concrètement leur souveraineté.

C'est en partie une question technique. Oui, les Premières Nations ont besoin de compétences techniques, d'éducation, de formation, etc. Mais c'est aussi culturel. Les Premières Nations doivent avoir assez d'espace pour exprimer leurs besoins en matière de gouvernance de l'information et des données de façon culturellement et linguistiquement pertinente. Mais en toile de fond, il faut voir que nombre de ces questions pourraient être résolues par l'application de la législation déjà adoptée par le gouvernement fédéral (préambules, déclarations publiques, traités et ententes), qui affirme le statut des gouvernements des Premières Nations en tant que gouvernements souverains ayant la capacité juridique de prendre le contrôle de leurs propres ressources, y compris en matière de données et d'information. Donc, selon moi, le principal obstacle qui distingue les membres des Premières Nations des autres Canadiens dans ce domaine, c'est la capacité politique et juridique. (I01)

Les articles 3 et 4 de la Déclaration des Nations Unies sur les droits des peuples autochtones traitent du droit à l'autodétermination, et du droit de disposer des moyens de financer leurs activités et de poursuivre leurs objectifs de développement. Un certain nombre de participants au sondage et aux entrevues voyaient ces droits comme la pierre d'assise de l'autodétermination et de la souveraineté des données autochtones. Les participants ont décrit un certain nombre d'obstacles systémiques empêchant la reconnaissance de la souveraineté autochtone sur la collecte, la conservation et l'utilisation des données pour prendre des décisions ayant une incidence sur leur bien-être. L'un d'entre eux a fait référence à des obstacles législatifs et légaux qui prennent la forme d'un racisme institutionnel freinant l'avancement de la souveraineté des données autochtones. Un autre a fait remarquer que les autorités gouvernementales étaient prises de court par la souveraineté des données autochtones, un concept relativement récent.

J'ajouterai que la souveraineté des données autochtones, pour moi, semble être un concept récent et que nombre d'entités gouvernementales ne sont pas préparées à l'autoriser, ou commencent seulement à créer des mécanismes pour en permettre l'exercice. (I06)

Un autre participant a donné un exemple de cette absence de préparation en décrivant le manque de compréhension du gouvernement fédéral quant aux interlocuteurs avec qui établir et maintenir des relations de nation à nation. Cette difficulté d'identifier l'instance dirigeante autochtone appropriée perpétue la non-reconnaissance de la souveraineté autochtone.

Et c'est à cause de cette non-reconnaissance que les groupes autochtones se sont trouvés exclus de la prise de décisions relatives à la gouvernance des données.

Donc, vous comprenez, ma vision de la gouvernance des données et de la souveraineté des données commence par le règlement de ce déséquilibre. Mais si nous ne sommes même pas invités à la table, c'est vraiment préoccupant. (I04)

Au-delà de cette participation aux discussions sur les grands enjeux, les participants ont insisté sur la nécessité d'intégrer des décideurs autochtones dans ces processus. L'un d'entre eux a souligné cette nécessité en lien avec le processus du CCNGD, expliquant qu'au lieu d'être consultés sur la question des normes de gouvernance des données, les groupes autochtones devraient être impliqués dans la direction du processus de normalisation, en reconnaissance de leur autonomie gouvernementale.

Je commencerai simplement par faire un commentaire plus large sur la gouvernance des données en général et des parallèles avec la question climatique, c'est-à-dire que la majorité de la gouvernance à ces deux tables se fait sans le bénéfice de la présence des Premières Nations… vous savez, je trouve ironique que les Premières Nations n'aident pas à diriger l'ensemble du processus [du CCNGD] lui-même. Je pense que c'est représentatif des problèmes que rencontrent les Premières Nations quand elles cherchent à comprendre des processus qui ne respectent ni leur gouvernance, ni leur système de connaissances, ni leurs droits. (I04)

Malgré les obstacles législatifs qui les empêchent d'affirmer leur autorité sur les données, les groupes autochtones continuent à chercher des façons d'exercer cette autorité.

Donc, c'est en quelque sorte là qu'on se trouve en ce moment : nous voulons affirmer et exercer notre autorité sur nos données, mais le cadre législatif actuel crée des obstacles. C'est un aspect du problème; mais si on y réfléchit bien, on peut se demander, faut-il vraiment légiférer pour nous donner cette autorité? Y a-t-il d'autres façons pour nous d'affirmer et d'exercer cette autorité sans l'inscrire dans la loi? (I02)

Certains participants ont décrit l'émergence d'un certain degré de reconnaissance dans des cas précis où les instances provinciales et fédérales avaient conclu des ententes prévoyant le partage des responsabilités en matière de collecte et de gestion des données avec les gouvernements et les organisations autochtones. La section 4.3 en donne quelques exemples.

4.2.1.1 Capacité

La capacité des gouvernements et des organisations autochtones à diriger la collecte, l'administration, la conservation et la diffusion des données fait également partie des enjeux soulevés par les participants aux entrevues et au sondage. Cette capacité a été décrite en termes d'infrastructures, d'équipements, de ressources humaines, de formation, de technologie et de financement.

Les participants ont souligné un certain nombre de problèmes relatifs au manque d'équipement et de technologie nécessaires à la gouvernance de l'information chez les organisations et gouvernements autochtones. Ils ont expliqué que ces gouvernements font appel à tout un éventail de méthodes, certains employant uniquement des documents papier alors que d'autres disposent de technologies plus modernes. Cette disparité de moyens entre les différents gouvernements (et à l'intérieur de chacun d'eux) pourrait causer la perte ou le compartimentage de données.

À cause de la vitesse à laquelle les technologies tombent en désuétude, un certain nombre d'organisations se retrouvent avec des données dans un format inutilisable ou inaccessible. Cela a été notamment souligné par les participants des régions du Nord.

D'abord, il y a globalement les piètres méthodes et infrastructures de données chez nous. L'ensemble des Territoires du Nord-Ouest connaît des limites importantes. Nous prenons des mesures pour changer les choses, mais nous sommes toujours loin derrière les meilleurs – comme la Colombie-Britannique ou l'Ontario – selon moi. (I06)

Un participant a expliqué que même s'il conduit avec une organisation inuite des recherches dirigées par les Autochtones, la capacité et l'infrastructure de stockage et de gestion des données ne suffisent pas à combler les besoins. Les participants qui travaillent dans le Nord, notamment dans les Territoires du Nord-Ouest et au Yukon, ont également souligné les difficultés de recrutement : un taux de roulement élevé et le peu de ressources en éducation et en formation nuisent à la capacité d'administrer et de gérer les données efficacement.

Un participant a expliqué que dans les Premières Nations de sa région du Nord, on manque de formation sur la façon d'utiliser et d'administrer des données. Les répondants au sondage ont également souligné la nécessité d'améliorer la formation pour rehausser l'habileté numérique des communautés autochtones.

Les répondants au sondage et les principaux participants ont souligné que la formation, le personnel, l'infrastructure et l'équipement nécessaires pour administrer et gérer les données coûtaient cher, et que de nombreuses communautés autochtones n'avaient pas le financement à long terme nécessaire pour installer et entretenir ces systèmes. L'un d'entre eux a indiqué que le renforcement des capacités de gestion des données au sein des gouvernements autochtones cédait le pas à d'autres problèmes, plus urgents, comme l'amélioration des conditions de vie. Deux participants ont décrit le rôle essentiel du financement à long terme pour permettre à leurs organisations d'améliorer leur capacité au point de pouvoir élaborer des stratégies et des politiques sur la collecte, l'administration et l'utilisation des données.

En tant qu'organisation, il nous manque depuis plusieurs années la capacité de vraiment élaborer une stratégie complète sur les données... pour élaborer une telle stratégie qui nous permettrait de faire avancer la souveraineté et la gouvernance des données et de créer un protocole de consultation. (Samantha Michaels)

De nombreux participants au sondage et aux entrevues ont insisté sur la nécessité d'un investissement fiable à long terme dans la capacité des communautés autochtones à exercer leur souveraineté sur les données.

Mais s'il y avait une chose sur laquelle le rapport devrait insister, je pense que ce devrait être la nécessité d'investir dans la capacité des Premières Nations à assurer la souveraineté des données; c'est vraiment le meilleur moyen d'avancer pour atteindre l'autonomie gouvernementale. (I07)

Je veux simplement ajouter… une partie du processus concerne la façon dont nous investissons à l'échelle communautaire pour faire les choses au bon niveau. Et souvent, il s'agit en partie de s'assurer que les communautés peuvent être autonomes, et n'ont pas à s'appuyer sur les autres. (I04)

4.2.1.2 Accès aux données

Les participants aux entrevues et au sondage ont insisté sur le fait que les gouvernements et organisations autochtones n'ont pas accès à l'information concernant leurs populations. Cette information étant hébergée par des chercheurs, des gouvernements ou d'autres organisations, les décideurs autochtones manquent des données nécessaires pour gouverner. Un participant a exprimé sa frustration devant ce manque d'accès aux données.

Et moi, je pense que pour de nombreuses raisons – mais je ne comprends pas pourquoi – la personne autochtone, le gouvernement autochtone, la collectivité autochtone ne sont pas aussi appréciés que leurs vis-à-vis non autochtones. Les autres obtiennent l'information beaucoup plus rapidement. Il y a même un processus, celui des demandes d'accès à l'information. Les citoyens peuvent demander toutes sortes de comptes; comme ce n'est pas vrai pour nous, les Autochtones, on peut se demander si nous avons autant de valeur comme citoyens. (I07)

Certains participants ont fait remarquer que la législation québécoise en particulier restreignait parfois l'accès aux données. Un autre participant a donné l'exemple d'un projet de recherche qu'il a mené avec une organisation autochtone sur les populations autochtones vulnérables et l'application de la loi, où l'accessibilité et la propriété des données ont dû être négociées avec les organismes d'application de la loi, entre autres ceux du gouvernement fédéral.

Dans certains cas, l'accès aux données est conditionnel au respect de certaines conditions. Un participant a décrit une expérience où l'accès aux données nécessaires n'était accordé qu'une fois que la capacité de l'organisation autochtone avait atteint un niveau suffisant, reconnu par les autorités fédérales et territoriales – un processus long et coûteux.

La deuxième difficulté, je pense, c'est qu'une organisation doit avoir une grande capacité et faire des investissements importants si elle veut obtenir l'accès aux données autochtones. Surtout pour les questions plus délicates, comme les données sur la santé. Il faut démontrer au gouvernement que vous avez la capacité d'administrer ces données. Il y a la continuité, il y a l'infrastructure, il y a les politiques. Tout doit être en place, ça coûte cher et c'est long. C'est compliqué. Il y a de nombreuses dispositions à respecter. Ça, c'est un obstacle vraiment important. (I06)

Des répondants au sondage se sont dits frustrés de voir des données autochtones diffusées et vendues par des utilisateurs secondaires sans supervision appropriée alors même qu'ils constatent les difficultés qu'ont les groupes autochtones pour accéder à leurs données.

4.2.1.3 Respect de la culture

Comme nous l'avons mentionné à la section 2.2, une grande partie de la collecte et de la recherche de données menées au Canada ne correspond pas aux besoins et aux priorités des communautés autochtones, et les données ont été extraites de ces communautés à de nombreuses reprises. Les participants à la consultation ont également affirmé que la collecte de données devait être dirigée par des organisations autochtones et que les méthodes de collecte et d'administration des données devaient refléter le contexte culturel, les valeurs et les normes propres aux Autochtones pour chaque projet.

Sur cette question, un répondant a souligné que les comités d'éthique en recherche cherchent davantage à gérer les risques qu'à s'assurer que les travaux sont menés de façon appropriée pour une certaine communauté. Un autre participant a donné un exemple de recherche médicale menée sur les Premières Nations de la Nouvelle-Écosse qui contrevenait aux valeurs de la communauté; comme le processus d'examen éthique n'avait pas impliqué cette communauté dans sa prise de décision, les travaux ont été menés sans supervision autochtone. Un autre participant a mis en lumière l'historique de l'extraction de données dans l'Inuit Nunangat.

... [dans] les quatre régions de l'Inuit Nunangat, je veux dire avant, les chercheurs pouvaient venir sans rien demander à personne, et d'une certaine façon exploiter la population ou nuire aux individus, ou faire des recherches bien sûr importantes pour une université ou pour une chose ou une autre, peu importe, mais avaient-elles une quelconque importance pour la population et lui étaient-elles utiles de quelque façon que ce soit? (Samantha Michaels)

Ces antécédents ont soulevé des préoccupations chez les populations autochtones quant à la nature des données collectées et diffusées. Selon un participant, cela nuit à la relation de confiance, même lorsque la collecte de données est menée par des Autochtones. Un répondant au sondage a souligné la nécessité de bâtir la confiance pour que les collectes de données menées par des Autochtones obtiennent le soutien des communautés.

La nécessité de reconnaître la science et les manières d'être et d'apprendre autochtones comme des moyens et méthodes plus adéquats pour la collecte de l'information sur les groupes autochtones a été soulevée par un grand nombre de participants au sondage et aux entrevues. Ces derniers ont exprimé leur frustration devant le mépris et le rejet des systèmes de connaissances autochtones, ainsi que devant l'utilisation constante de paramètres scientifiques occidentaux mal adaptés à un contexte autochtone.

Ces grands enjeux ne concernent pas seulement la souveraineté des données en ce qui touche la protection de l'information, mais aussi la souveraineté et l'autonomie pour faire accepter votre science et votre façon d'être et d'acquérir des connaissances. Pas nécessairement validées, mais acceptées et sur le même pied que les normes scientifiques et les façons occidentales d'analyser les données. (I07)

J'imagine que c'est comme un microcosme des grands défis de gouvernance des données sur la façon dont on s'assure que c'est contrôlé et dirigé par les Premières Nations en fonction de la combinaison des différents systèmes de connaissances et univers où elles évoluent; mais comment s'assure-t-on que les processus menant aux résultats sont vraiment menés par ces mêmes Premières Nations? Sinon, on risque essentiellement de perpétuer le modèle du manque de respect envers les connaissances, la science et l'innovation des Premières Nations. (I04)

Les répondants ont insisté sur l'importance de ne pas extraire les données de leur contexte culturel et de ne pas les détacher des protocoles et processus autochtones associés.

... Lorsqu'on détache les données de l'endroit, on peut les manipuler comme on veut et je pense que c'est vraiment problématique en regard des principes autochtones sur les données. Comment rendons-nous des comptes à une communauté? Quels sont les protocoles et processus nécessaires? Parce qu'une fois les données détachées du contexte, elles sont sorties du système où elles fonctionnent. (I04)

Un participant a insisté sur le fait qu'en abolissant les obstacles législatifs, il fallait faire place à la création et à l'utilisation de paramètres et de normes définis par les Autochtones en ce qui regarde les données. Le potentiel de ces paramètres et de ces normes pour l'amélioration du bien-être autochtone, grâce à l'autodétermination, a été mis en lumière par un certain nombre de participants.

Je crois que le plus important, c'est d'aplanir les obstacles à la souveraineté des données. Je pense que cela signifie que le gouvernement fédéral, les personnes qui font les normes, les provinces et les autres partenaires de la Confédération doivent vraiment investir dans la capacité des Premières Nations à faire ce travail. Les obstacles sont dans les lois, mais aussi dans les normes elles-mêmes. Il n'y a pas d'espace pour que les Premières Nations hébergent l'information, utilisent leurs propres paramètres. (I07)

4.3 NORMES ET INITIATIVES EXISTANTES

Les participants ont mentionné un certain nombre de normes et d'initiatives pertinentes pour l'élaboration de normes canadiennes sur la gouvernance des données, qui affirment la souveraineté des peuples autochtones sur tous les aspects de la collecte, de la gestion et de l'utilisation de leurs données. Les normes et initiatives dirigées par des Autochtones – mentionnées lors de la consultation ou repérées grâce à une brève revue de la littérature – sont décrites aux sections 4.3.1 à 4.3.3. Voici une brève description de quelques initiatives et organisations jugées pertinentes par les participants.

- Dans le domaine de la santé autochtone, un certain nombre d'initiatives ont découlé de partenariats et d'ententes de partage des données conclus avec les autorités fédérales, provinciales ou territoriales pour permettre aux groupes autochtones de mener la collecte et l'administration des données. En voici quelques exemples : l'Autorité sanitaire des Premières Nations de la Colombie-Britannique; l'unité de la Stratégie de recherche axée sur le patient des Territoires du Nord-Ouest Hotìı ts'eeda; le comité de gouvernance de la recherche sur les données de santé du Secrétariat à la santé et au développement social des Premières Nations du Manitoba; et le Service des projets de données et de gouvernance de l'information de l'Union of Nova Scotia Mi'kmaq (UNSM).
- Le Centre de gouvernance de l'information des Premières Nations mène un certain nombre d'initiatives et a produit tout un éventail de ressources liées à la gouvernance des données autochtones (dont les exemples donnés aux sections 4.3.1 et 4.3.3).
- La Commission de la santé et des services sociaux des Premières Nations du Québec et du Labrador a publié le *Cadre de référence sur la gouvernance de l'information des Premières Nations au Québec* et travaille actuellement à sa mise en œuvre.
- L'Initiative de gouvernance des données des Premières Nations de la Colombie-Britannique a été créée pour mener des projets de démonstration afin d'établir la gouvernance et la souveraineté des données autochtones.

4.3.1 Principes de PCAP®

Au Canada, ce sont les Premières Nations qui sont à l'origine des pratiques contemporaines de souveraineté des données autochtones. En 1998, le Comité directeur national (CDN) de l'Enquête régionale longitudinale sur la santé des Premières Nations et des Inuits a établi un ensemble de normes sur l'éthique des données pour garantir aux Premières Nations le contrôle et la gouvernance de la collecte, la diffusion, la propriété et l'utilisation des données les concernant. Les principes de propriété, de contrôle, d'accès et de possession (PCAP®) des Premières Nations définissent la collecte, l'utilisation et la conservation éthiques des données des Premières Nations dans le respect de leurs visions du monde respectives. Le Centre de gouvernance de l'information des Premières Nations (CGIPN) détient la marque de commerce PCAP® au bénéfice de toutes les Premières Nations. Les principes de PCAP® ont été conçus pour refléter les valeurs, les protocoles et les pouvoirs des Premières Nations quant à la souveraineté des données. Bien que de nombreuses organisations et administrations inuites et métisses aient adopté des protocoles et des principes semblables, les principes de PCAP® ne constituent pas une norme panautochtone sur la souveraineté des données.

Les principaux participants ont insisté sur le fait que les principes de PCAP® des Premières Nations expriment une souveraineté qui relève d'une relation de nation à nation avec le gouvernement fédéral.

Les principes de PCAP® doivent être compris et respectés par tous, y compris le gouvernement fédéral : ils donnent aux Premières Nations l'espace nécessaire pour assurer la gouvernance des données comme elles le souhaitent et exercer leur souveraineté sur ces données selon leur propre vision du monde. Mais c'est vraiment très difficile de faire comprendre aux gens [extérieurs aux Premières Nations] que leur rôle dans la mise en œuvre des principes de PCAP® doit s'inscrire dans cette vision de la souveraineté. Il ne s'agit pas seulement d'avoir une éthique solide, de bien communiquer ou d'avoir de bonnes intentions. La souveraineté s'exerce dans le contexte particulier des lois sur la propriété intellectuelle, des différentes autorités, de toute l'histoire de la relation constitutionnelle entre les Premières Nations et le gouvernement fédéral. (I01)

...comment passer de processus dirigés par le fédéral ou le provincial où les Premières Nations sont invitées à commenter, à des travaux menés par les Premières Nations elles-mêmes? Vous savez, les principes de PCAP® sont un genre de manifestation de ce transfert de pouvoir aux Premières Nations pour leur permettre de promouvoir leurs propres intérêts et priorités. (I04)

Les participants au sondage et aux entrevues ont décrit des occasions où les principes de PCAP® ont été ignorés parce que les organisations utilisant des données des Premières Nations avaient négligé de reconnaître l'autorité de celles-ci, l'avaient mal interprétée ou l'avaient carrément écartée. Malgré tout, les participants ont insisté sur le fait que les principes de PCAP® conservent leur importance et leur pertinence en tant qu'expression de la souveraineté des données des Premières Nations.

Nous sommes propriétaires des inventions qui relèvent de notre propriété intellectuelle. Pour obtenir des renseignements de notre communauté, il faut passer par ce processus. Il a été contourné par le passé, à répétition. Les gens se disaient « C'est juste une résolution adoptée par une organisation autochtone qui a une certaine autorité, il y a une structure de gouvernance qui donne des dents à cette résolution, mais ce n'est pas dans la loi. Nous pouvons contrevenir aux principes de PCAP® et demander pardon après, plutôt que de demander la permission avant ». (I07)

Les principes de PCAP® n'ont pas été gravés dans la pierre en 1998; ils sont vivants, ils évoluent. Tout comme les conceptions et les pratiques entourant la possession de données ont évolué en 2021, les principes de PCAP® peuvent évoluer aussi tout en gardant leur pertinence. (I01)

Bon, il s'agit de gouvernance des Premières Nations à l'ère numérique, ok. À quoi ça ressemble exactement? Ça reste à préciser. Mais c'est un défi que doivent maintenant relever les principes de PCAP®, je pense. Cette idée de possession, de rétention des droits de propriété et de tout ce que ça implique, sur quelque chose d'aussi éphémère que des données. C'était probablement le cas dans les années 1990, mais encore plus de nos jours. (I01)

4.3.2 Stratégie de gouvernance des données des Premières Nations

En mars 2020, le Centre de gouvernance de l'information des Premières Nations a présenté à Services aux Autochtones Canada un rapport intitulé *Stratégie de gouvernance des données des Premières Nations* (SGDPN) qui propose une avenue réaliste vers la souveraineté des données pour les Premières Nations. Cette stratégie définit deux priorités stratégiques à court terme : 1) la création d'équipes de champions des données dans chaque région et à l'échelle nationale; 2) un financement provisoire pour les travaux de préparation à la mise en œuvre. Le CGIPN et ses partenaires prépareront une analyse de rentabilité nationale pour obtenir un financement éventuel dans le budget 2021.

La SGDPN est fondée sur des principes axés « sur les collectivités et les nations ». Elle établit neuf piliers d'action décrivant les priorités en matière de capacités de données des Premières Nations. Elle comprend un plan progressif de mise en œuvre, un modèle de maturité et un cadre de responsabilité. Il importe de souligner que la Stratégie est une initiative de transformation des systèmes complexe et multidimensionnelle et qu'elle explore un territoire vierge où les jalons et les expériences sont rares. Elle a l'ambition d'établir un réseau de dix centres régionaux semi-autonomes et un centre national de gouvernance de l'information dirigés par les Premières Nations dans l'ensemble du pays, selon la vision des détenteurs de droits. La Stratégie donne des arguments solides en faveur d'un tel réseau, et en démontre concrètement les effets à court, moyen et long terme.

Certains participants ont insisté sur l'importance de la SGDPN comme document d'orientation sur les étapes que doivent franchir les nations pour exercer leur souveraineté sur leurs données.

Donc, à la base, le scénario est le suivant : onze centres statistiques dirigés par les Premières Nations dans l'ensemble du pays, dix régionaux et un national, où les détenteurs de droits des Premières Nations (communautés, Nations et dirigeants) contrôlent complètement les données grâce à la gouvernance de leur centre régional d'information ou de statistique. La structure de gouvernance de chaque centre devrait refléter celle des Nations de la région. (I02)

Ces centres seront également dotés de l'expertise, des capacités et des infrastructures nécessaires, au même niveau que les autres centres statistiques du pays – comme Statistique Canada. La création d'institutions des Premières Nations ne signifie pas la disparition des institutions existantes. (I02)

Chaque centre régional de gouvernance des données créé dans la foulée de la SGDPN serait ancré dans les valeurs, les langues et la notion de propriété collective des Premières Nations.

À l'approche de la mise en œuvre, nous devons étudier la façon dont nous pouvons arriver à la propriété collective et au contrôle de nos données. Rien dans la législation actuelle n'y est favorable. La Loi sur la protection des renseignements personnels*, par exemple, protège les individus; il faudrait la revoir pour y intégrer des protections collectives. (I02)*

Les participants ont également souligné l'importance de prévoir un financement continu à long terme pour bâtir les capacités nécessaires à l'application de la SGDPN.

Donc, la volonté politique c'est une chose, mais la capacité réelle de faire avancer les choses en est une autre. Cette stratégie sur les données, dans le fond, c'est un plan progressif sur dix ans pour bâtir la capacité de gouvernance et trouver les ressources humaines pendant que nous avançons les autres dossiers. (Gwen Phillips)

4.3.3 Stratégie nationale inuite sur la recherche

En 2018, l'adoption de la Stratégie nationale inuite sur la recherche (SNIR) visait la refonte des pratiques de recherches dommageables adoptées par des acteurs externes aux communautés de l'Inuit Nunangat. La SNIR établit un ensemble de principes de recherche qui affirment la gouvernance inuite sur la façon dont les données et l'information sur les Inuits, la faune et l'environnement sont collectées, conservées, utilisées et diffusées. Elle insiste sur le fait que les chercheurs externes doivent communiquer avec les Inuits d'une façon qui reconnaît leur autonomie gouvernementale et leur autodétermination. La SNIR affirme également que toutes les recherches menées sur les Inuits, la faune et l'environnement doivent l'être de façon à bénéficier aux Inuits. Elle comporte deux grandes parties :

1. Une description de la vision inuite de la recherche et du lien étroit entre la recherche inuite et un objectif global d'équité sociale et économique pour les Inuits.
2. Cinq secteurs prioritaires visant la gouvernance par les Inuits des données et de l'information recueillies pendant les recherches dans l'Inuit Nunangat.

Le quatrième secteur prioritaire – *Assurer l'accès, la propriété et le contrôle des Inuits relativement aux données et à l'information* – est particulièrement pertinent. Le plan de mise en œuvre de la SNIR en décrit les livrables, de même que les principaux décideurs et partenaires impliqués dans la poursuite de cet objectif dans la période de cinq ans couverte. Un certain nombre de comités de l'Inuit Tapiriit Kanatami (ITK), dont le Comité national de l'Inuit Qaujisarvingat (CNIQ) et le Comité national inuit sur la gestion des données, sont au cœur de cette mise en œuvre.

4.4 L'AVENIR DE LA GOUVERNANCE DES DONNÉES AUTOCHTONES

Si des initiatives comme la SGDPN et la SNIR tracent une voie claire vers la gouvernance et la souveraineté des données pour les Premières Nations et les Inuits respectivement, les participants ont aussi fait état d'un certain nombre d'éléments généraux qu'ils aimeraient retrouver dans l'avenir de la gouvernance des données autochtones et des normes connexes.

De manière générale, ils ont insisté sur le fait que la souveraineté des données fait partie intégrante d'un mouvement plus large vers l'autodétermination, et en constitue l'une des premières étapes.

Vous savez, je ne fais pas de distinction entre les aspirations en matière de gouvernance et de souveraineté des données et le projet plus large que représente l'autodétermination des Premières Nations. Parce que je pense que les difficultés et les objectifs de la défense de la souveraineté des données autochtones correspondent aussi à la défense de l'autodétermination autochtone, et de celle des Premières Nations en particulier. (I04)

Les relations de nation à nation au moyen d'ententes de partage de données ont été présentées comme des moyens importants de faire avancer la souveraineté des données et l'autodétermination autochtones. Les normes relatives à la gouvernance des données autochtones devraient être basées sur ces relations.

Mais ce qui est primordial dans cette histoire de normalisation, c'est de réfléchir à la vraie relation qui sous-tend les normes. Il ne faut donc pas chercher à généraliser l'exercice. (Gwen Phillips)

Pour créer et maintenir ces relations, les participants ont souligné la nécessité pour les administrations fédérales, provinciales et territoriales de se donner les moyens de mieux comprendre les peuples autochtones et dialoguer avec eux, par exemple en améliorant leurs compétences culturelles et leur compréhension de l'histoire de la gouvernance des données autochtones.

La dernière chose que je voudrais – c'est bizarre... Ça semble impossible, mais le gouvernement fédéral devrait améliorer sa capacité de comprendre les peuples autochtones et de dialoguer avec eux. Et je dirais que c'est un contexte semblable pour la gouvernance des données, il doit comprendre ce que signifient la gouvernance et la souveraineté des données autochtones, et vous savez, toute l'histoire, etc. (I04)

L'établissement et le maintien de relations entre les instances dirigeantes autochtones sur la création de systèmes de gestion des données font également partie des conditions importantes mises de l'avant par les participants pour assurer l'interopérabilité et éviter les dédoublements.

Il est possible de collaborer et de construire un système de gestion des données qui répond aux besoins de tous et améliore l'interopérabilité, le partage entre les Premières Nations afin que nous ne réinventions pas continuellement la roue et que nous soyons mieux en mesure de participer à la cogestion et à la mise en œuvre des ententes finales. (I11)

L'avenir de la gouvernance des données que décrivent les participants fait une large place aux lois, normes et indicateurs de qualité définis et administrés par des gouvernements autochtones autodéterminés, qui reflètent les valeurs et les systèmes de connaissances autochtones. L'un des participants au sondage les juge essentiels à la collecte de meilleures données et à l'instauration d'un climat de confiance et de responsabilité envers les citoyens.

Nous savons qu'il faut des normes. Et la définition de la qualité en est l'un des éléments les plus importants. (Gwen Phillips)

Nous devons réfléchir stratégiquement pour donner aux institutions le pouvoir de favoriser la reconstruction de la Nation. Encore une fois, il faut avoir confiance dans les données et disposer d'une stratégie globale et de normes. (Gwen Phillips)

Et quand nous étudions la question dans l'optique des façons d'apprendre des Autochtones ou des Premières Nations, cela inclut nos langues, nos récits, nos cérémonies, nos chants, nos pictogrammes, selon l'endroit où on se trouve. Il faut donc clarifier ce qui constitue des données dans ce contexte, je pense que c'est vraiment important. (I04)

Pour les répondants au sondage, les spécialistes de la gouvernance des données et leaders autochtones devront suivre des formations sur l'application des normes définies par les Autochtones. Les participants ont également souligné que toutes les autres personnes touchées par le cycle de vie des données à différents ordres de gouvernement, du fédéral au municipal, devraient aussi suivre une formation sur les rôles et responsabilités de chacune des parties. Un participant a également évoqué la nécessité potentielle de créer des normes professionnelles pour les personnes qui géreront les données autochtones, de même que le besoin d'agents autochtones de protection des renseignements personnels pour surveiller l'application des normes.

5. Recommandations

5.1 RECOMMANDATIONS

En nous basant sur les commentaires recueillis pendant la consultation, nous formulons ici des recommandations quant à la poursuite de la consultation et à la participation des gouvernements et organisations autochtones au processus du CCNGD.

1. Impliquer davantage les organisations et les experts en gouvernance des données inuits et métis. Étant donné leur faible participation à la consultation, il faut poursuivre les travaux pour connaître le point de vue de ces importants groupes autochtones sur les questions de gouvernance des données et sur les travaux du CCNGD.
2. Impliquer davantage les gouvernements et organisations autochtones dans le processus du CCNGD pour consacrer suffisamment de temps et de ressources à une définition claire des enjeux soulevés par les gouvernements et organisations autochtones et à leur intégration, le cas échéant, aux enjeux déjà définis par les groupes de travail du CCNGD. Cela peut notamment se traduire par la participation de représentants autochtones aux groupes de travail du CCNGD. Par exemple, un certain nombre d'enjeux définis par le groupe de travail 1 qui ont obtenu un classement élevé au sondage, dont les *directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique*, le *cadre des responsabilités* et la *gouvernance de la gestion des données*, devront faire l'objet d'une rétroaction supplémentaire de la part des peuples autochtones.
3. Au moyen d'autres consultations, repérer les principales organisations autochtones (notamment celles qui s'occupent déjà de l'élaboration de normes ou de principes, comme l'Inuit Tapiriit Kanatami et le Centre de gouvernance de l'information des Premières Nations respectivement) en vue de les impliquer dans les prochaines étapes des travaux du CCNGD, y compris la normalisation elle-même.

5.2 CONCLUSION

Si vous souhaitez discuter de n'importe quel aspect du présent rapport, n'hésitez pas à communiquer avec Guy Polden, au Groupe Firelight.

Tél. : 778 851-0264
Courriel : guy@firelight.ca

Bibliographie

Centre de gouvernance de l'information des Premières Nations (CGIPN). « First Nations Data Sovereignty in Canada », *Statistical Journal of the IAOS*, vol. 35, n° 1 (2019), p. 1-23. https://doi.org/10.3233/SJI-180478.

Centre de gouvernance de l'information des Premières Nations (CGIPN). *Ownership, Control, Access and Possession (OCAP®): The Path to First Nations Information Governance*, 2014.

Centre de gouvernance de l'information des Premières Nations (CGIPN). « Pathways to First Nations' Data and Information Sovereignty », *Indigenous Data Sovereignty: Toward an Agenda*, Tahu Kukutai et John Taylor (dir.), p. 139-155, Acton (Australie), ANU Press, 2016.

Commission de vérité et réconciliation du Canada (CVR). *Rapport final de la Commission de vérité et réconciliation du Canada*, 2015.

Commission royale sur les peuples autochtones (CRPA). *Rapport de la Commission royale sur les peuples autochtones*, 1996.

Espey, J. *« Stewardship and OCAP: A Discussion Paper for the First Nations. Statistical Institute »*, Institut de la statistique des Premières nations, mai 2002. Inuit Tapiriit Kanatami (ITK). *Stratégie nationale inuite sur la recherche*, 2018.

Kukutai, Tahu et John Taylor (dir.). *Indigenous Data Sovereignty: Toward an Agenda*, Acton (Australie), ANU Press, 2016.

Lovett, Raymond, Vanessa Lee, Tahu Kukutai, Donna Cormack, Stephanie Rainie et Jennifer Walker. « Good data practices for indigenous data sovereignty and governance », *Good Data*, Angela Daly, S. Kate Devitt et Monique Mann (dir.), p. 26-36, Institute of Network Cultures, 2019.

McBride, Kate. *Data Resources and Challenges for Nations Communities*, Alberta First Nations Information Governance Centre (AFNIGC), 2018.

McMahon, Rob, Trevor James Smith et Tim Whiteduck. « Reclaiming Geospatial Data and GIS Design for Indigenous-led Telecommunications Policy Advocacy: A Process Discussion of Mapping Broadband Availability in Remote and Northern Regions of Canada », *Journal of Information Policy*, vol. 7 (2017), p. 423-449.

Raine, Stephanie C., Jennifer. L. Schultz, Elleen Briggs, Patricia Briggs et Nancy Lynn Palmanteer-Holder. « Data as a Strategic Resource: Self-determination, Governance, and the Data Challenge for Indigenous Nations in the United States », *International Indigenous Policy Journal,* vol. 8, n° 2 (2017), p. 1-29.

Raine, Stephanie C., Tahu Kukutai, Maggie Walter, Oscar Luis Figueroa-Rodríguez, Jennifer Walker et Per Axelsson. « Indigenous data sovereignty », The *State of Open Data – Histories and Horizons*, Tim Davies, Stephen B. Walker, Mor Rubinstein et Fernando Perini (dir.), p. 300-319, African Minds, IDRC, 2019.

Smith, Diane E. « Governing data and data for governance: the everyday practice of Indigenous sovereignty », *Indigenous Data Sovereignty: Toward an Agenda*, Tahu Kukutai et John Taylor (dir.), p. 117-135, Acton (Australie), ANU Press, 2016.

Snipp, C. Matthew. « What Does Data Sovereignty Imply: What Does It Look Like? » *Indigenous Data Sovereignty: Toward an Agenda*, Tahu Kukutai et John Taylor (dir.), p. 39-56, Acton (Australie), ANU Press, 2016. [consulté le 25 février 2021]

Steffler, Jeanette. « The Indigenous Data Landscape in Canada: An Overview », *Aboriginal Policy Studies,* vol. 5, n° 2 (2016), p. 145-164.

Annexe 1 : Formulaire de consentement pour l'entrevue

CONSULTATION AUTOCHTONE SUR LES TRAVAUX DU COLLECTIF CANADIEN DE NORMALISATION EN MATIÈRE DE GOUVERNANCE DES DONNÉES – ENTREVUE AVEC LES PRINCIPAUX PARTICIPANTS

Consentement éclairé et autorisation d'utiliser l'information

Je soussigné(e), (nom) _____ , le (date complète) _____ , autorise Firelight Research Inc. à mener une entrevue avec moi dans le cadre de la Consultation autochtone sur les travaux du Collectif canadien de normalisation en matière de gouvernance des données.

Je comprends que l'entrevue est menée par Firelight Research Inc. et que l'étude a pour objectif de recueillir les commentaires préliminaires de groupes autochtones sur les enjeux de gouvernance des données propres aux Inuits, aux Métis et aux Premières Nations afin de connaître les points de vue autochtones sur la façon d'aborder ces enjeux et les initiatives existantes en matière de gouvernance et de souveraineté des données autochtones.

Par ma signature, je confirme que :

1. je consens à voir mes paroles et mes réponses consignées par écrit et dans l'enregistrement (Zoom);
2. je comprends que je peux refuser de répondre aux questions et mettre fin à l'entrevue à n'importe quel moment;
3. je comprends que les personnes qui participent à cette recherche restent propriétaires des réponses qu'elles donnent lors des entrevues. Chacune d'elles recevra l'enregistrement et la transcription de l'entrevue et conservera les droits sur ceux-ci. Les participants recevront le rapport qui découlera de l'étude; ils pourront le passer en revue et modifier la façon dont leurs propos sont cités ou interprétés avant la publication. Toutes les données seront conservées sur un serveur protégé situé au Canada, dont Firelight est propriétaire et gestionnaire, et seront détruites au plus tard un an après avoir été recueillies.

Pour information, communiquer avec Guy Polden au 604 345-7532.

J'accepte que mes paroles soient citées dans le rapport. Je comprends que je peux retirer mon consentement ultérieurement : **oui** **non**

J'accepte que mon nom soit mentionné dans le rapport. Je comprends que je peux retirer mon consentement ultérieurement : **oui** **non**

Signature _____

Témoin _____

NIP :

Annexe 2 : Sondage

Ce sondage est effectué par le Groupe Firelight au nom du Collectif canadien de normalisation en matière de gouvernance des données (CCNGD). Firelight s'adresse à des représentants, des détenteurs de connaissances et des experts en gouvernance de données autochtones pour connaître le point de vue autochtone sur la gouvernance de données, en vue de l'élaboration de la feuille de route du CCNGD.

Le Collectif canadien de normalisation en matière de gouvernance des données

Créé en 2019 pour coordonner la définition de stratégies normatives en matière de gouvernance des données au Canada, le CCNGD n'a pas pour mandat de rédiger des normes, mais plutôt de permettre aux parties prenantes d'optimiser leurs ressources, de faire état de leurs besoins, de proposer une coordination des travaux normatifs et de minimiser les redondances quant aux questions relatives à la gouvernance des données au Canada.

Les normes de gouvernance des données renvoient aux pratiques exemplaires qui encadrent la collecte, l'utilisation, la conservation, l'archivage, le transfert, la suppression et l'élimination des données. La feuille de route du CCNGD décrira l'état actuel de la gouvernance des données au Canada et les objectifs à poursuivre, en plus de cerner les lacunes à combler, de formuler des recommandations à cet égard, de définir des priorités d'action et de proposer des organisations pour l'élaboration des normes de gouvernance des données.

Le sondage

Le sondage est la première des deux phases du processus : Firelight s'adresse à des représentants, des détenteurs de connaissances et des experts en gouvernance des données autochtones pour connaître leur point de vue sur l'intégration des perspectives autochtones dans les stratégies de gouvernance des données. Les renseignements fournis par les participants en réponse au sondage serviront à rédiger un rapport sur la gouvernance des données autochtones à l'intention du CCNGD. La phase 2, qui commencera à l'été 2020, tablera sur les résultats de la phase 1.

Accord de consentement

La participation au sondage est entièrement volontaire. Vous pouvez refuser de participer à la recherche ou quitter le processus à tout moment sans conséquence. Vous pouvez refuser de répondre à toute question, peu importe la raison. Les renseignements fournis sont tout à fait confidentiels.

Ce sondage est réalisé par le Groupe Firelight. Firelight est une compagnie autochtone qui mène des études participatives auprès des communautés autochtones de tout le Canada depuis plus de dix ans. Pour mieux connaître Firelight, consulter son site Web au https://firelight.ca.

Coordonnées

Si vous avez des questions sur le projet, communiquez avec Guy Polden (guy.polden@firelight.ca).

À ce jour, le CCNGD a exploré 35 grands enjeux liés à la gouvernance des données. Nous aimerions connaître les points de vue autochtones sur dix de ces grands enjeux; les autres seront explorés à la phase deux. Les questions porteront sur les éléments suivants :

1. Recherches actuelles : personnes ou organisations menant des recherches sur chacun des enjeux
2. Priorités : enjeux de gouvernance des données à prioriser
3. Lacunes : aspects à améliorer pour l'élaboration des normes de gouvernance des données autochtones
4. Recommandations : façons d'améliorer la gouvernance des données, mesures à prendre
5. Recherche et développement : personnes ou organisations qui devraient s'occuper de la recherche et du développement pour les normes de gouvernance des données autochtones

PARTIE 1

1. Les enjeux de la gouvernance des données autochtones varient d'une population à une autre. Nous désirons nous assurer que les informations recueillies sont représentatives des perspectives de l'ensemble des communautés. Veuillez indiquer les populations autochtones dont vous traitez ou avez traité les données.
   - ☐ Premières Nations
   - ☐ Inuits
   - ☐ Métis
   - ☐ Autres (veuillez préciser)
2. Dans quels secteurs travaillez-vous?
   - ☐ Santé
   - ☐ Justice
   - ☐ Gouvernance
   - ☐ Gestion des ressources naturelles
   - ☐ Technologies de l'information
   - ☐ Finances
   - ☐ Autre (veuillez préciser)

PARTIE 2

Pour la prochaine série de questions, nous vous demandons quelle importance vous accordez à dix enjeux de gouvernance des données; ce qui nous intéresse, c'est le point de vue autochtone à cet égard.

Après avoir brièvement expliqué chaque enjeu, nous vous demandons de lui donner une importance sur une échelle de 1 à 5 (de 1 : pas important à 5 : très important).

Cadre des responsabilités

Cet enjeu concerne la structure de responsabilité et de contrôle pour toutes les données créées ou recueillies et décrit les rôles et responsabilités en matière de traitement des données. La responsabilité du détenteur des droits sur les données, les conséquences d'un transfert de propriété et la notion de consentement sont également abordées.

3. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives au cadre de responsabilité dans l'élaboration des normes sur la gouvernance des données autochtones?
   - ☐ Très important
   - ☐ Important
   - ☐ Assez important
   - ☐ Peu important
   - ☐ Pas important

Attestations encadrant les rôles professionnels

Cet enjeu concerne le rôle des professionnels qui traitent les données et l'information et explore les programmes de certification à créer de même que les besoins de l'industrie. Il devrait d'abord aborder l'évaluation des exigences de compétences professionnelles en fonction d'un cadre clair constituant la colonne vertébrale de la gouvernance des données.

4. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives aux attestations encadrant les rôles professionnels dans l'élaboration des normes sur la gouvernance des données autochtones?

Habileté numérique

Cet enjeu concerne l'habileté numérique, et plus particulièrement l'amélioration de la compréhension des données, des technologies et des interfaces par la population canadienne. L'habileté numérique doit être distinguée des attestations professionnelles et avoir une portée plus large, incluant l'utilisation efficace et sécurisée des technologies. L'éducation est un outil important pour sensibiliser les Canadiens aux difficultés et aux avantages d'une société de plus en plus numérique, ce qui est nécessaire pour la mise en place d'un cadre de gouvernance des données efficace et inclusif.

5. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives à l'habileté numérique dans l'élaboration des normes sur la gouvernance des données autochtones?
   - ☐ Très important
   - ☐ Important
   - ☐ Assez important
   - ☐ Peu important
   - ☐ Pas important

Cybersécurité et protection des données

Cet enjeu couvre la cybersécurité, la protection des données et la transparence, éléments transversaux d'un cadre de gouvernance des données. Les menaces évoluent en même temps que les outils technologiques, et il nous faudra des mécanismes plus élaborés pour protéger les données et les renseignements sensibles. Les principaux risques pour la cybersécurité concernent l'infrastructure numérique, de réseau et de connectivité.

6. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives à la cybersécurité et à la protection des données dans l'élaboration des normes sur la gouvernance des données autochtones?
   - ☐ Très important
   - ☐ Important
   - ☐ Assez important
   - ☐ Peu important
   - ☐ Pas important

Gouvernance de la gestion des données

Cet enjeu explore la nécessité de planifier, superviser, surveiller et appliquer la gestion des données à l'échelle organisationnelle, et vise à expliciter la manière de gérer les données tout au long de leur cycle de vie. L'enjeu devrait couvrir l'élaboration, l'exécution et la supervision de plans, de politiques, de programmes et de pratiques visant à contrôler, à protéger, à assurer et à améliorer la valeur des données et des actifs d'information. Il devrait également prévoir un cadre qui permettrait l'examen de la gestion des données à l'échelle organisationnelle.

7. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives à la gouvernance de la gestion des données dans l'élaboration des normes sur la gouvernance des données autochtones?
   - ☐ Très important
   - ☐ Important
   - ☐ Assez important
   - ☐ Peu important
   - ☐ Pas important

Protection des renseignements personnels

Cet enjeu explore la nécessité de planifier, superviser, surveiller et appliquer la gestion des données à l'échelle organisationnelle, et vise à expliciter la manière de gérer les données tout au long de leur cycle de vie. L'enjeu devrait couvrir l'élaboration, l'exécution et la supervision de plans, de politiques, de programmes et de pratiques visant à contrôler, à protéger, à assurer et à améliorer la valeur des données et des actifs d'information. Il devrait également prévoir un cadre qui permettrait l'examen de la gestion des données à l'échelle organisationnelle.

8. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives à la protection des renseignements personnels dans l'élaboration des normes sur la gouvernance des données autochtones?
   - ☐ Très important
   - ☐ Important
   - ☐ Assez important
   - ☐ Peu important
   - ☐ Pas important

Directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique

L'enjeu explore la fiabilité et l'éthique dans l'utilisation des données, conformément aux attentes canadiennes quant aux renseignements personnels énoncés dans la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection des renseignements personnels*. Il vise à clarifier les aspects éthiques de la propriété ou de la gérance des données, ainsi que leur utilisation éthique et sociale en fonction de leur valeur publique. Il faudrait mieux comprendre ce qu'il faut aux propriétaires, aux gardiens et aux fournisseurs de données ainsi qu'au public pour être dignes de confiance dans la collecte, la gestion, la conservation et l'utilisation de ces données, et pour démontrer activement leur fiabilité tout au long du cycle de vie des données.

9. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives aux directives sur la fiabilité et l'éthique dans le traitement des données et leur utilisation publique dans l'élaboration des normes sur la gouvernance des données autochtones?
   - ☐ Très important
   - ☐ Important
   - ☐ Assez important
   - ☐ Peu important
   - ☐ Pas important

Données ouvertes et procédures d'harmonisation et d'interopérabilité des données

Cet enjeu explore la nécessité de planifier, superviser, surveiller et appliquer la gestion des données à l'échelle organisationnelle, et vise à expliciter la manière de gérer les données tout au long de leur cycle de vie. L'enjeu devrait couvrir l'élaboration, l'exécution et la supervision de plans, de politiques, de programmes et de pratiques visant à contrôler, à protéger, à assurer et à améliorer la valeur des données et des actifs d'information. Il devrait également prévoir un cadre qui permettrait l'examen de la gestion des données à l'échelle organisationnelle.

10. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives aux données ouvertes et aux procédures d'harmonisation et d'interopérabilité des données dans l'élaboration des normes sur la gouvernance des données autochtones?
    - ☐ Très important
    - ☐ Important
    - ☐ Assez important
    - ☐ Peu important
    - ☐ Pas important

Rôle des acteurs et des opérations de traitement des données

Cet enjeu couvre le rôle des différents acteurs tout au long du cycle de vie de la chaîne d'approvisionnement. De la collecte à l'utilisation des données interviennent une multitude de processus de traitement. Peu importe la quantité de données, de nombreuses personnes sont impliquées, qu'il s'agisse de les protéger contre les accès non autorisés ou de faire des sauvegardes quotidiennes, par exemple. Ces acteurs sont responsables de protéger les données par la création d'un système sécurisé qui réduit les risques d'erreurs. L'enjeu souligne donc la responsabilité des professionnels des données et leurs obligations.

11. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives au rôle des acteurs et des opérations de traitement des données dans l'élaboration des normes sur la gouvernance des données autochtones?
    - ☐ Très important
    - ☐ Important
    - ☐ Assez important
    - ☐ Peu important
    - ☐ Pas important

Réutilisation des données

Cet enjeu couvre la réutilisation des données, c'est-à-dire une utilisation qui n'était pas prévue à l'origine et qui vise un objectif différent de celui qui a été accepté par le détenteur des droits sur les données et pour lequel il n'a pas donné de consentement explicite.

12. Sur une échelle de 1 à 5, quelle importance accordez-vous aux questions relatives à la réutilisation des données dans l'élaboration des normes sur la gouvernance des données autochtones?
    - ☐ Très important
    - ☐ Important
    - ☐ Assez important
    - ☐ Peu important
    - ☐ Pas important

PARTIE 3

La dernière série de questions porte sur les travaux actuellement menés par des organisations autochtones sur la gouvernance des données.

13. Y a-t-il d'autres enjeux relatifs à la gouvernance des données autochtones qui ne figurent pas ici?
    - ☐ Oui
    - ☐ Non

14. Si oui, lesquels?

_____

_____

15. À votre connaissance, d'autres recherches sont-elles actuellement menées sur l'élaboration de normes de gouvernance des données autochtones?
    - ☐ Oui
    - ☐ Non

16. Si oui, par qui?

_____

_____

17. Quel est l'objet de ces recherches?

_____

_____

18. Connaissez-vous des normes sur la gouvernance des données autochtones qui pourraient s'appliquer à l'échelle nationale?
    - ☐ Yes
    - ☐ No

19. Si oui, veuillez nous en parler.

_____

_____

20. Connaissez-vous des personnes ou des organisations qui seraient aptes à élaborer des normes de gouvernance des données d'un point de vue autochtone?
    - ☐ Yes
    - ☐ No

21. Si oui, lesquelles?

_____

_____

Merci d'avoir répondu au sondage!

Annexe 3 : Guide d'entrevue

CONSULTATION AUTOCHTONE SUR LES TRAVAUX DU COLLECTIF CANADIEN DE NORMALISATION EN MATIÈRE DE GOUVERNANCE DES DONNÉES – GUIDE D'ENTREVUE AVEC LES PRINCIPAUX PARTICIPANTS

Contenu :

- Contexte de l'étude
- Questions d'entrevue

Présentation

Firelight s'adresse aux organisations, représentants et experts en gouvernance des données autochtones pour recueillir leurs points de vue sur la gouvernance et la souveraineté des données autochtones. Cette information servira à formuler des recommandations pour l'élaboration de la feuille de route du Collectif canadien de normalisation en matière de gouvernance des données (CCNGD). Notre recherche vise à recueillir les commentaires préliminaires de groupes autochtones sur les enjeux de gouvernance des données propres aux Inuits, aux Métis et aux Premières Nations, à décrire les normes autochtones actuelles sur la gouvernance des données (p. ex. les principes de PCAP®) ainsi que les points de vue autochtones sur la façon d'aborder ces enjeux. Le rapport faisant état des résultats de la recherche alimentera l'élaboration de la feuille de route du CCNGD; il traitera séparément des enjeux propres aux Inuits, aux Métis et aux Premières Nations et formulera une série de recommandations basées sur les commentaires et les conseils recueillis.

Contexte

Qu'est-ce que la gouvernance des données?

La gouvernance des données est un concept vaste, mais il s'agit essentiellement de la structure (personnes, organisations et processus) mise en place pour prendre des décisions sur la collecte, la gestion, la conservation, la récupération et la communication des données.

Qu'est-ce que le Collectif canadien de normalisation en matière de gouvernance des données?

Créé en 2019 pour coordonner la définition de stratégies normatives en matière de gouvernance des données au Canada, le CCNGD n'a pas pour mandat de rédiger des normes, mais plutôt de permettre aux parties prenantes d'optimiser leurs ressources, de faire état de leurs besoins, de proposer une coordination des travaux normatifs et de minimiser les redondances quant aux questions relatives à la gouvernance des données au Canada

Les normes de gouvernance des données renvoient aux pratiques exemplaires qui encadrent la collecte, l'utilisation, la conservation, l'archivage, le transfert et l'élimination des données. La feuille de route du CCNGD, rédigée par quatre groupes de travail intersectoriels, décrira l'état actuel de la gouvernance des données au Canada et les objectifs à poursuivre, en plus de cerner les lacunes à combler, de formuler des recommandations à cet égard, de définir des priorités d'action et de proposer des organisations pour l'élaboration des normes de gouvernance des données.

Les groupes de travail ont cerné un certain nombre d'enjeux, mais comme ils ne comptent aucun représentant de groupes autochtones, notre recherche vise à obtenir les commentaires préliminaires des Inuits, des Métis et des Premières Nations sur les enjeux de gouvernance des données autochtones.

Voici les principales questions auxquelles nous cherchons à répondre :

- En matière de gouvernance des données, quels sont actuellement les principaux enjeux pour les groupes autochtones du Canada?
- Quelles normes existantes portent sur la gouvernance et la souveraineté des données autochtones?
- Dans l'idéal, quel serait l'avenir de la gouvernance et de la souveraineté des données autochtones selon les groupes des Premières Nations, des Inuits et des Métis?
  - Comment y arriver?
  - Qui devrait participer au processus?
- Quel devrait être le rôle des normes sur les données dans cet avenir idéal?

Utilisation de l'information recueillie

Chaque participant (sondage ou entrevue) doit donner son consentement éclairé. Les renseignements communiqués par les participants dans le cadre de l'étude serviront à rédiger un rapport sur la gouvernance des données autochtones à l'intention du CCNGD. Ce rapport formulera une série de recommandations basées sur les réponses des participants, notamment sur la façon dont les groupes autochtones pourraient s'investir dans la suite du processus.

Cette étude préliminaire vise à cerner les enjeux préoccupants quant à la gouvernance des données autochtones. Il faudra poursuivre les recherches pour approfondir la question, et pour décider s'il est pertinent d'élaborer des normes de gouvernance des données autochtones. Ces recherches seront menées en fonction des recommandations formulées dans le rapport, conformément aux pratiques exemplaires établies par les experts et leaders du domaine autochtones.

[Lire ce qui suit au début de chaque entrevue, après avoir lancé l'enregistrement.]

Nous sommes le [date]. Nous menons une entrevue avec [nom du participant ou de la participante] dans le cadre de la Consultation autochtone sur les travaux du Collectif canadien de normalisation en matière de gouvernance des données effectuée par Firelight. Merci de votre présence. Je m'appelle [nom], et voici mon/ma/mes collègue(s) [nom(s)]. Nous menons cette entrevue grâce au logiciel de vidéoconférence Zoom. [Nom du participant] a lu et signé le formulaire de consentement, et nous lui avons attribué le numéro d'identification [NIP]. Nous lui avons expliqué l'objectif de l'étude et le plan d'entrevue.

1. **Contexte**
   - Décrivez-nous brièvement votre travail, et en quoi cela concerne la gouvernance des données autochtones.
2. **Enjeux de gouvernance des données**
   - En matière de gouvernance des données, quels sont actuellement les principaux enjeux pour les groupes autochtones du Canada?
   - Sur quels enjeux faut-il se concentrer tout particulièrement?
   - Selon vous, ces enjeux sont-ils différents pour les groupes des Inuits, des Premières Nations et des Métis?
3. **Normes et initiatives existantes**
   - Quelles normes existantes portent sur la gouvernance et la souveraineté des données autochtones?
   - Quelle est l'efficacité de ces initiatives quant aux enjeux de la gouvernance des données autochtones?
   - Quels obstacles nuisent à l'efficacité de ces normes et initiatives?
   - Quel rôle jouent ces normes et initiatives dans le renforcement de la souveraineté et de la gouvernance des données autochtones?

4. **Avenir**
   - Dans l'idéal, quel serait l'avenir de la gouvernance et de la souveraineté des données autochtones?
   - Comment y arriver?
   - Qui devrait participer au processus?
   - Selon vous, quel devrait être le rôle des normes sur les données dans cet avenir idéal?

Conclusion

[Lire ce qui suit à la fin de chaque entrevue, ***avant d'arrêter l'enregistrement*** *audio et vidéo.]*

Nous sommes le [date]. Nous venons de terminer l'entrevue avec [nom du participant ou de la participante] dans le cadre de la Consultation autochtone sur les travaux du Collectif canadien de normalisation en matière de gouvernance des données effectuée par Firelight.

Je m'appelle [nom], et voici mon/ma/mes collègue(s) [nom(s)]. Nous avons mené cette entrevue sur Zoom. L'entrevue a duré environ [nombre] heures [nombre] minutes.

Annexe 4 : Matériel promotionnel

MÉDIAS SOCIAUX (TEXTE)

Facebook/LinkedIn

Les collectes de données au sujet des peuples autochtones du Canada et l'utilisation des informations recueillies demeurent trop souvent déficientes et inadéquates. Plusieurs Premières Nations, ainsi que les Inuits, Métis et autres groupes autochtones visent à atteindre la souveraineté des données. Les décisions concernant les normes de gouvernance des données ne peuvent être prises sans une collaboration étroite avec les groupes autochtones. Firelight Group travaille en collaboration avec le Conseil canadien des normes afin de mener un sondage et de poser la question suivante : Quelles sont les principales problématiques de la gouvernance des données?

Visitez le https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey pour répondre au sondage et courez la chance de remporter une carte-cadeau de 100 $ au magasin de votre choix.

Contactez Guy Polden de chez Firelight pour plus de détails.
Courriel : guy.polden@firelight.ca

Anglais

There is a long history of poor data collection and misuse of information collected about Indigenous populations in Canada. Currently, many First Nations, Inuit, Metis and other Indigenous groups and organisations are striving towards the concept of data sovereignty. Decisions on data governance standards cannot be made without the close involvement of Indigenous groups. The Firelight Group is working with the t to conduct a survey that asks: What are the main data governance issues or challenges that Indigenous groups currently face?

Visit https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey to complete the survey. Fill out the survey for the chance to win a $100 gift card to the business of your choice!

Questions? Contact Guy Polden at The Firelight Group.
Email: guy.polden@firelight.ca

Twitter

Firelight Group travaille en collaboration avec le Conseil canadien des normes afin de mener un sondage et de poser la question suivante : Quelles sont les principales problématiques de la gouvernance des données?

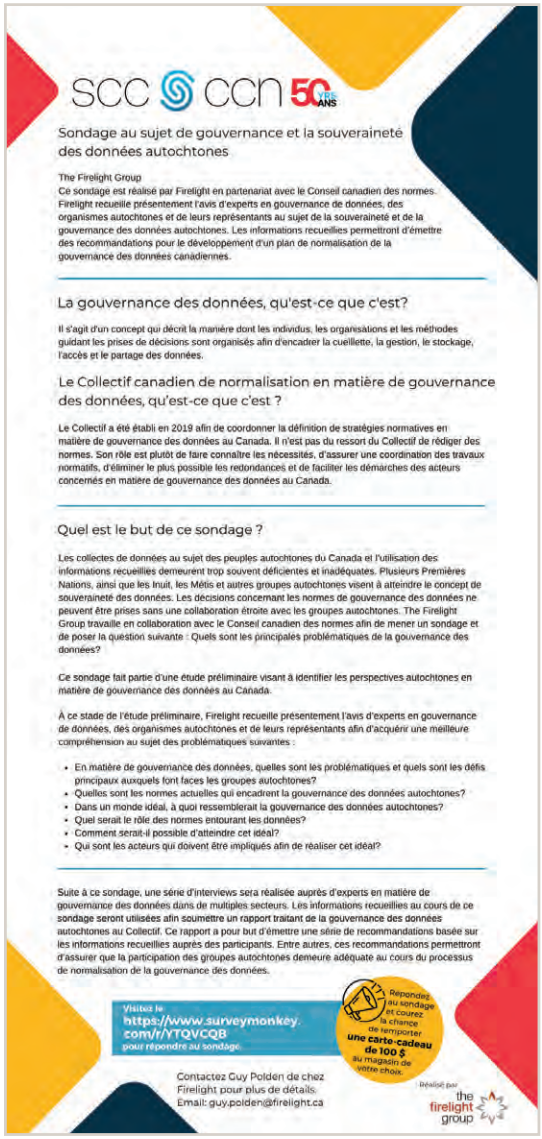
Visitez le https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey pour répondre au sondage et courez la chance de remporter une carte-cadeau de 100 $ au magasin de votre choix.

Anglais

The Firelight Group is working with the Canadian Data Governance Standardization Collaborative to conduct a survey that asks: What are the main data governance issues or challenges that Indigenous groups currently face?

Visit https://www.surveymonkey.com/r/RoadmapDevelopmentSurvey to complete the survey. Fill out the survey for the chance to win a $100 gift card to the business of your choice!

MÉDIAS SOCIAUX (GRAPHISME)



Annexe D –

Cas d'usage

Cas d'usage n° 1 – Données sur la santé communautaire

Contexte

Des initiatives à l'appui de la santé communautaire et du besoin de normalisation ont récemment vu le jour partout au pays. Pensons entre autres à celle du Réseau des travailleurs et travailleuses en santé communautaire du Canada, qui vise à appuyer les travailleurs du domaine[21] et à stimuler le développement de la santé communautaire d'un océan à l'autre. Comme les travailleurs en santé communautaire sont « ancrés dans les communautés qu'ils servent et sensibles aux nombreuses difficultés que ces dernières éprouvent »[22], il est important que les secteurs public et privé travaillent de concert pour créer un environnement sûr, sécuritaire et fiable pour la santé communautaire au Canada. Il faut faire des données sur la santé communautaire une priorité pour les décideurs, les politiciens et les dirigeants d'entreprise afin que le gouvernement établisse des politiques en la matière, de même que pour faire le pont entre les différents établissements de santé (surtout en ce qui concerne l'interopérabilité des données sur la santé communautaire et la prestation de soins virtuels) et pour satisfaire les membres des diverses communautés du Canada.

DONNÉES SUR LA SANTÉ COMMUNAUTAIRE ET NORMALISATION

Dans un contexte de normalisation de la gouvernance des données, les dossiers médicaux et les données sur la santé correspondent aux renseignements recueillis sur les patients et transmis entre les fournisseurs de soins et leurs partenaires. En santé – caractéristique unique au domaine –, les données ont la double utilité de bénéficier directement aux patients, mais aussi à la communauté élargie. L'art de la gouvernance des données, c'est ici de trouver dans chaque situation l'équilibre entre les besoins des uns et des autres. Le Collectif de normalisation en matière de gouvernance des données, dans le cadre de son cas d'usage des données sur la santé communautaire, a examiné les aspects de la gouvernance impliqués dans la transmission de dossiers médicaux et de données sur la santé aux participants du système de soins au moyen de dossiers médicaux électroniques (DME), dans le contexte de la COVID-19.

21 Réseau des travailleurs et travailleuses en santé communautaire du Canada. https://www.chwnetwork.ca/index.php?option=com_content&view=article&id=27&Itemid=108

22 Réseau des travailleurs et travailleuses en santé communautaire du Canada. https://www.chwnetwork.ca/index.php?option=com_content&view=article&id=27&Itemid=108

Les dossiers médicaux et les données sur la santé fournissent des renseignements précieux sur la santé de la population. Il est donc nécessaire d'établir des normes pour harmoniser la tenue des dossiers médicaux au Canada, car les normes actuelles (ex. : concernant la vaccination ou les résultats diagnostiques) diffèrent d'un endroit à l'autre. Il existe également des divergences dans les normes régissant la collecte des renseignements médicaux et leur transmission entre les fournisseurs de soins et leurs partenaires. Compte tenu du fait que « la santé numérique offrira sa pleine valeur seulement lorsque les systèmes d'information sur la santé seront tous interreliés et [qu'on pourra] y accéder facilement afin de s'échanger de l'information »[23], cet enjeu est non négligeable.

Les normes sur les données de santé sont un volet essentiel de l'interopérabilité. Les normes pancanadiennes devront fournir le langage technique et les termes cliniques permettant aux fournisseurs de soins de santé de tout le pays de communiquer et d'échanger des renseignements médicaux de manière sûre, fiable et cohérente. Appliquées à des solutions numériques en santé, ces normes : 1) aideront les membres des équipes de soins à bien interpréter et à échanger les renseignements nécessaires à la prestation de soins sûrs et efficaces; 2) faciliteront la prise de décisions cliniques grâce à des alertes et à des rappels; et 3) permettront de regrouper les données (sous réserve des approbations requises) à des fins de recherche clinique dans le but d'améliorer les résultats de santé[24].

La création d'un seul modèle de DME pour remédier aux irrégularités des données sur la santé nécessiterait l'évaluation de tous les modèles existants pour choisir celui à adopter, après consultation des personnes concernées (p. ex. professionnels de la santé et patients). Les DME constituent une précieuse ressource en santé communautaire, car les dossiers des patients, surtout ceux des visiteurs d'autres provinces, sont souvent incomplets et manquent d'uniformité. Si les normes en matière de données et de dossiers médicaux diffèrent d'un endroit à l'autre, c'est qu'au Canada, les soins de santé sont une compétence provinciale. Il est donc très difficile pour les fournisseurs de soins, leurs partenaires, voire les patients eux-mêmes d'obtenir des antécédents médicaux complets et détaillés. En raison des retards que cela cause dans l'accès aux renseignements, les patients risquent de recevoir un mauvais diagnostic ou de subir des effets secondaires évitables[25].

Considérons les dossiers médicaux et les données sur la santé sous l'angle de la COVID-19. Tout le monde peut recevoir des vaccins : ils sont utiles à l'échelle individuelle pour prévenir les maladies et dans la population pour prévenir les éclosions. Dans le système d'éducation, la vaccination sert même de critère d'entrée. Ainsi, les enjeux liés à l'absence de normalisation des dossiers médicaux ont eu de grandes répercussions sur les Canadiens; toujours dans le système d'éducation, des milliers d'élèves ont reçu des avis de renouvellement de vaccins et des centaines d'autres ont été suspendus en attendant leur vaccination. Au moment de la vaccination contre la COVID-19, cette question deviendra primordiale.

La nécessité de normaliser les dossiers médicaux, compte tenu de l'importance particulière des données sur la santé, varie selon leur utilité pour les acteurs du secteur de la santé : la santé publique cherche à garder la population en bonne santé; les décideurs de la santé veulent déterminer le financement nécessaire à une vaccination efficace; les décideurs de l'éducation visent à protéger leur population; et le secteur privé cherche à vendre des vaccins efficaces. En parallèle, les chercheurs utilisent les données pour évaluer et accroître l'efficacité de la vaccination et des méthodes ou isoler les cas lors d'une éclosion, et les autorités de réglementation cherchent à protéger le droit des individus de revendiquer la propriété de leurs données.

23 https://www.infoway-inforoute.ca/fr/solutions/interoperabilite-clinique-et-normes-d-information-sur-la-sante
24 https://www.infoway-inforoute.ca/fr/solutions/interoperabilite-clinique-et-normes-d-information-sur-la-sante
25 https://www.cbc.ca/radio/whitecoat/a-national-electronic-health-record-for-all-canadians-1.4976932

Pour tenir compte des points d'intersection de la gouvernance et des données sur la santé touchant la COVID-19, il faut uniformiser la terminologie médicale et favoriser l'interopérabilité entre les systèmes concernés. Cela permettrait, entre autres, de mieux comprendre les données sur la santé, par exemple pour la vaccination : les systèmes pertinents pourraient, ensemble, nous indiquer quels vaccins immunisent contre quelles maladies avec quels médicaments. Cette démarche mènerait en quelque sorte à un portail de données sur la santé et éviterait les complications résultant de déménagements interprovinciaux, de changements de principaux fournisseurs de soins, etc. Il faut également se pencher sur l'accès aux données et sur le couplage et la confidentialité de celles-ci, afin de déterminer qui peut y accéder avec consentement et qui peut y accéder sans consentement. Il faut aussi songer à permettre l'analyse de ces données, laquelle a le potentiel de permettre à la communauté médicale élargie d'évaluer l'efficacité de vaccins et leurs effets secondaires. Les acteurs de la communauté médicale doivent également se demander si les données sur la santé devraient servir à influencer les comportements, notamment par l'envoi de rappels et d'avis de disponibilité relatifs à la vaccination.

La création de DME interopérables fournira à chaque Canadien un dossier d'antécédents médicaux et de soins de santé sûr, confidentiel et accessible. Axer cette création sur l'interopérabilité facilitera le partage de données entre les organismes de soins de santé et les régions, facilitera l'accès aux services de santé, et améliorera la qualité des soins, la sécurité des patients et l'efficacité, économisant temps et argent au système de santé[26].

Séances de discussion sur les données de santé communautaire

Les 9, 11 et 14 décembre 2020, le Conseil canadien des normes (CCN) et le Collectif canadien de normalisation en matière de gouvernance des données ont animé des séances de discussion avec le public sur les données de santé communautaires. De ces séances, deux étaient en anglais et une en français. Elles ont attiré plus de 23 participants de partout au pays, dont des fonctionnaires, des conseillers stratégiques, et des représentants de compagnies spécialisées dans la sécurité des données et d'associations et d'agences médicales et de soins de santé.

Au début de chaque séance, les représentants du CCN ont effectué une courte présentation sur le rôle du Collectif, l'importance des normes et l'état actuel des données de santé au Canada. Les participants ont ensuite été invités à s'exprimer sur les deux grands thèmes suivants :

- l'**état actuel** des données de santé communautaire au Canada, notamment les droits d'accès à ces données ainsi que leurs domaines d'utilisation et de non-utilisation;
- l'**avenir idéal** du domaine au Canada, notamment les règles, les règlements ou les normes nécessaires à l'encadrement des données de santé.

ÉTAT DES LIEUX ET DÉFIS ACTUELS

À l'occasion d'un exercice d'introduction interactif autour d'un tableau blanc, les participants ont cerné trois grands problèmes concernant les données de santé communautaire du Canada :

1. l'absence de normes relativement aux données et à la terminologie;
2. le manque d'intégration entre les fournisseurs de soins de santé, ce qui se traduit notamment par une fragmentation de l'information;
3. les grandes différences dans les lois provinciales et territoriales qui limitent le couplage des données.

26 https://www.infoway-inforoute.ca/fr/solutions/fondements-de-la-sante-numerique/dossiers-de-sante-electroniques/dse-interoperable

Au terme de l'exercice, les participants ont échangé en petits groupes, notant plusieurs obstacles à l'accès aux données de santé au Canada, dont le fait que les dossiers médicaux ne soient pas numérisés, l'impossibilité pour les patients d'obtenir ou de transmettre leur propre dossier, et le manque d'intégration des systèmes de données qui complique le partage des rares données numérisées entre les professionnels de la santé. Les normes sur la saisie des données médicales font défaut dans le système de soins, si bien qu'il en est difficile de surveiller les tendances de santé publique ou l'efficacité des traitements et des politiques sanitaires. Les patients ne sont souvent pas en mesure de saisir les renseignements qu'ils recueillent eux-mêmes à l'aide des nouvelles technologies comme les montres intelligentes, dont l'exactitude et l'utilité sont par ailleurs remises en cause en raison du vide normatif qui les entoure. Les participants ont également convenu que la plupart des patients et des professionnels de la santé comprennent mal les règles actuelles encadrant les données de santé au Canada, et que ces règles ne permettent pas aux patients de donner facilement leur consentement éclairé à l'égard de la transmission et de l'utilisation de leurs renseignements médicaux personnels.

AVENIR IDÉAL

Les participants prônent une plus grande interopérabilité des données de santé au Canada, afin que patients et professionnels disposent de données de santé partageables, normalisées et de grande qualité, et que les patients puissent plus facilement recevoir des traitements médicaux en dehors de leur province ou territoire de résidence et se les faire rembourser. Les patients devraient avoir le contrôle sur leurs propres données médicales, pouvoir les utiliser où et quand ils en ont besoin, et être en mesure d'y ajouter des données de santé normalisées recueillies grâce aux nouvelles technologies. Il faut instaurer de solides mécanismes pour assurer la sécurité des données de santé et en garantir l'inviolabilité, et tout consentement à la transmission de ces données doit être motivé par un objectif et avoir une durée de validité précise. Les patients et les professionnels de la santé devraient être mieux formés sur les règles actuelles régissant les données de santé et sur les normes à venir dans ce domaine. Les participants souhaitent que les données de santé puissent circuler de façon transparente entre les systèmes, les provinces et territoires, les fournisseurs et les patients afin d'assurer l'équité des soins au Canada, indépendamment du lieu de résidence.

DISCUSSIONS

État des lieux des données de santé communautaire

Au cours de la première partie des discussions en petits groupes, les participants ont été invités à dresser un état des lieux des données de santé communautaire au Canada.

Q1.1 : Quel est l'état actuel des données de santé communautaire au Canada (qui a accès à ces données, où sont-elles utilisées, et où pourraient-elles l'être)?

Thème n° 1 : Accès aux données

Plusieurs participants ont souligné l'existence d'obstacles à l'accès aux données médicales au Canada. Plus précisément, la plupart des notes échangées entre médecins ou avec les patients sont manuscrites, ce qui complique la transmission et la traçabilité des renseignements. De plus, les patients n'ont pas accès aux dossiers médicaux que tiennent leur médecin de famille, leurs spécialistes ou leurs autres fournisseurs de soins de santé. Ce problème se fait particulièrement sentir lorsqu'un patient change de médecin (p. ex. lors du départ à la retraite de son médecin de famille), reçoit des soins en dehors de sa province de résidence ou souhaite obtenir un suivi médical dans sa province après avoir reçu un premier traitement ailleurs.

Les participants ont également mentionné les difficultés de communication des données entre les hôpitaux et les cabinets et cliniques privés et entre la santé publique et les services médicaux d'urgence, plusieurs faisant observer que l'on croit souvent à tort que les systèmes de données sont interreliés. Cette lacune est devenue plus criante pendant la pandémie : les solutions numériques servant à collecter et stocker les données sur les contacts et les contaminations possibles se sont multipliées, sans qu'il y ait de système réglementé pour transmettre et utiliser les renseignements.

Les participants ont aussi évoqué l'incertitude qui plane sur la propriété des données de santé d'un patient et leur devenir si ce dernier est frappé d'une invalidité ou décède.

Par ailleurs, la sécurité des données de santé suscite des inquiétudes, plusieurs participants ayant signalé que les bases de données peuvent facilement être divulguées ou piratées.

Thème n° 2 : Point de saisie

Le moment et le lieu de saisie des informations sur la santé ont fait l'objet de vives discussions. Les participants ont fait remarquer qu'avec les nouvelles technologies, telles que les dispositifs portables comme les Fitbits ou les montres intelligentes, les données de santé peuvent désormais être collectées en dehors de l'écosystème de santé traditionnel (cliniques, hôpitaux), directement par les patients. Toutefois, bon nombre de ces dispositifs portables n'ont pas été conçus dans une optique de sécurité, et les données qu'ils recueillent ne sont ni réglementées ni normalisées, ce qui remet en question leur exactitude et leur utilité. Les participants ont aussi souligné que, même lorsque ces données sont fiables, il peut être difficile de les transmettre aux fournisseurs de soins de santé.

Faute de normes sur la saisie des données dans l'écosystème traditionnel des soins, il est difficile de surveiller les tendances de santé publique ou de mesurer l'efficacité des traitements et des politiques de santé communautaire. Comme l'a affirmé un participant, « il conviendrait de mieux encadrer la saisie des données ».

Thème n° 3 : Confidentialité et consentement

Les participants ont fait valoir que le Canada dispose d'un solide cadre juridique en matière de protection des renseignements personnels, appliquant les normes les plus rigoureuses au monde en matière de consentement. De manière générale, il existe deux types de consentement pour la collecte et l'utilisation des données personnelles : le consentement présumé et le consentement demandé. Au Canada, c'est le premier qui prime. Cela dit, les participants ont estimé qu'il pouvait être difficile d'établir des normes de confidentialité pour les données de santé, surtout quand il n'existe pas de règlement sur l'utilisation secondaire des données collectées. D'autres participants ont indiqué que certains formulaires de consentement sont trop longs ou difficiles à comprendre, ce qui ne permet pas aux patients d'exprimer un consentement éclairé quant à l'utilisation des données de santé personnelles qu'ils transmettent et laisse planer le doute quant à la durée de validité de ce consentement ou son devenir en cas d'invalidité ou de décès.

En outre, en l'absence de normes de sécurité rigoureuses ou de protocoles de consentement transparents, les nouvelles technologies et les dispositifs portables permettant aux patients de recueillir eux-mêmes des données sur leur santé peuvent compromettre la confidentialité des renseignements.

Q1.2 : À votre connaissance, quels sont les règles, les règlements et les normes qui encadrent actuellement les données de santé?

Thème n° 4 : Mécompréhension des règles

De l'avis général, la plupart des patients et des professionnels de la santé comprennent mal les règles qui encadrent les données de santé au Canada. Par conséquent, il plane une incertitude sur les obligations concernant la collecte, le stockage et la transmission de ces données. Certains participants ont déclaré s'inspirer du Règlement général sur la protection des données (RGPD) de l'Union européenne ou des règles de protection des données en vigueur aux États-Unis, mais ces normes ont plutôt été élaborées pour encadrer des organisations privées et non le secteur public. Les participants ont convenu que les règles actuelles varient dans chaque province et territoire, ce qui peut compliquer les échanges de données de santé. Les participants ont également déploré le flou entourant les règles régissant la collecte et la transmission de données de santé par les dispositifs portables.

Avenir des données de santé communautaire

Au cours de la seconde partie des discussions en petits groupes, les participants ont été invités à se prononcer sur l'avenir souhaité pour les données de santé communautaire au Canada.

Q2.1 : Quel est l'avenir idéal des données de santé au Canada?

Thème nº 5 : Interopérabilité

L'interopérabilité a fait l'objet de nombreuses discussions, notamment en ce qui concerne la circulation des données entre les systèmes et les régions et par-delà les frontières, ainsi que la nécessité de la faciliter lors des mises à jour des systèmes de données sur la santé. Tous se sont entendus sur le fait que l'établissement de normes, en assurant une plus grande interopérabilité dans tout le pays, fournirait aux patients et aux professionnels de la santé des données médicales partageables, normalisées et de haute qualité. De nombreux participants ont déclaré vouloir un écosystème de la santé où patients et professionnels auraient accès, en tous lieux, à des renseignements fiables et exploitables au point d'intervention, de sorte que les fournisseurs de soins disposent de l'information la meilleure et la plus récente. À cette fin, il faudrait numériser les renseignements, dont les dossiers des patients actuellement conservés au format papier dans les cabinets de médecins, les cliniques et les autres points de service.

D'autres participants ont fait remarquer qu'une interopérabilité accrue simplifierait le système de données de santé en permettant aux provinces, aux territoires et au gouvernement fédéral d'échanger toute information pertinente, de même qu'elle faciliterait les démarches et le remboursement des patients soignés en dehors de leur province ou territoire de résidence.

Thème nº 6 : Accès aux données

Au-delà du consensus sur le fait que les fournisseurs de soins de santé et les partenaires du secteur devraient avoir un bien meilleur accès aux données de santé pour améliorer les soins et les résultats, une grande partie de la discussion sur l'accès aux données visait la capacité des patients à obtenir leurs propres données et les utiliser quand ils en ont besoin. Comme l'a fait remarquer un participant, « bon nombre de Canadiens n'ont pas de médecin de famille. Ces gens doivent avoir accès à leurs données pour pouvoir recevoir des soins quand ils en ont besoin ». Un autre participant a déclaré que, selon lui, les patients de demain seront les premiers responsables de la gestion de leurs données de santé.

Les participants souhaitent également que les patients aient la possibilité de transmettre aux fournisseurs de soins de santé les données qu'ils collectent grâce aux nouvelles technologies (p. ex. montres intelligentes, applications de conditionnement physique, moniteurs de fréquence cardiaque) pour que leurs dossiers soient aussi complets et à jour que possible. Un participant a fait l'observation suivante : « Une multitude de renseignements recueillis par ces appareils sont largement ignorés par les médecins. »

Thème nº 7 : Sécurité et consentement

Les participants ont jugé que la sécurité et la fiabilité des renseignements étaient deux volets essentiels à l'efficacité du système de données sur la santé, ce qui sous-entend de solides mesures de protection garantissant l'inviolabilité des renseignements et un contrôle strict des personnes pouvant accéder à une partie ou à la totalité des données. Un participant a déclaré que le consentement du patient qui autorise l'accès à ses données de santé devrait être motivé par un objectif qui déterminerait la durée de validité du consentement, et être explicite afin de susciter la confiance à l'égard du système. Les acteurs du secteur privé sont actuellement passibles d'une amende en cas de violation des règles sur la confidentialité, et le groupe a souligné que des sanctions similaires devront être appliquées dans le secteur public pour préserver la confiance dans la manière dont les administrations et organismes publics utilisent les données de santé. « Les Canadiens doivent savoir ce qu'il advient de leurs données et avoir leur mot à dire », a déclaré un participant.

Bien que le groupe ait estimé de façon générale que le patient devrait avoir le choix de transmettre ou non ses données de santé, certains participants se sont demandé si la gestion des risques ne serait pas le parent pauvre de la protection des renseignements personnels. Une personne s'est aussi demandé si la confidentialité pouvait parfois être sacrifiée sur l'autel du bien commun, car l'objectif principal de l'utilisation des données de santé devrait être d'améliorer à la fois le bien-être de chacun et celui de la communauté élargie.

Thème nº 8 : Formation et certification

Pour donner suite à un constat précédent – la plupart des patients et des professionnels de la santé comprennent mal les règles actuelles régissant les données de santé au Canada –, les participants ont convenu qu'il devrait y avoir plus de formation à ce sujet et une meilleure normalisation des règles. Le groupe a souligné que la normalisation ne freine pas l'innovation – fait démontré par de nombreuses autres professions, dont l'ingénierie, qui suivent des règles normalisées applicables à tous – et que ces règles peuvent évoluer et changer avec le temps. Quelqu'un a suggéré que les futures normes sur les données de santé fassent l'objet d'un cours obligatoire dans les collèges et les universités. Un autre participant a mentionné qu'il faudrait encourager les professionnels de la santé à demeurer au fait des normes sur les données de santé, peut-être en imposant cette condition au maintien de leur certification.

Q2.2 : Quel est l'avenir idéal des données de santé au Canada?

Thème nº 9 : Vision commune

Les participants ont souligné que la dimension humaine devrait toujours être au cœur des activités d'élaboration de normes sur les données de santé. Le système de soins devrait être simplifié pour faciliter les échanges de renseignements entre les provinces et territoires et avec les administrations fédérales. Il faudrait aussi articuler l'interopérabilité des données de santé autour d'une vision nationale commune : celle de données circulant sans heurt entre les systèmes, les provinces et territoires, les fournisseurs et les patients afin d'assurer des soins équitables peu importe le lieu de résidence. Le groupe a proposé qu'Inforoute Santé du Canada et d'autres organismes similaires contribuent à la réalisation de cette vision et d'une stratégie commune, et œuvrent à l'adoption de normes pancanadiennes sur les données de santé. Il a aussi suggéré l'adoption par le Canada d'un cadre de gouvernance des données et de l'information comme celui de l'Institut canadien d'information sur la santé. Les participants ont estimé que la mise en place de dispositifs réglementaires ou normatifs renforcerait la confiance des patients dans l'utilisation de leurs données de santé.

Rapport du groupe de travail sur le cas d'usage

APPROCHE

Le groupe travaillant sur le cas d'usage des données sur la santé communautaire a adopté une vision verticale des principaux enjeux étudiés par les différents groupes de travail du Collectif canadien de normalisation en matière de gouvernance des données. Il s'est inspiré du travail mené par Statistique Canada pour la création de sa plateforme CODAS (qui sert à collecter des données de multiples sources et à les mettre à la disposition de Statistique Canada et d'utilisateurs externes) et du Cadre de renforcement des compétences et de la gouvernance en matière de données et d'information sur la santé de l'Institut canadien d'information sur la santé (https://www.cihi.ca/fr/cadre-de-renforcement-des-competences-et-de-la-gouvernance-en-matiere-de-donnees-et-dinformation). Pendant les discussions sur le cycle de vie, plusieurs difficultés récurrentes ont été cernées et classées en trois thèmes.

Il est rapidement devenu apparent que ce cas d'usage s'étend bien au-delà des enjeux relatifs à la COVID-19 et qu'il fallait examiner l'entièreté de la chaîne d'approvisionnement des données, notamment les avantages de la normalisation pour la collecte et l'encodage des données au point d'origine; le rôle de l'échange de données et de l'interopérabilité pour permettre l'agrégation de données; et l'utilité de lignes directrices sur l'analytique et l'étude des données qui intègrent des principes d'éthique et de transparence pour stimuler l'action. Le groupe a donc établi un flux de données général pour représenter les processus d'étude des données en santé communautaire (impliquant la population, des fournisseurs de soins, des chercheurs et des décideurs). Il a aussi créé une architecture de politiques sur les données qui couvre la chaîne d'approvisionnement des données de bout en bout (voir la fin du rapport).

Les enjeux relevés par le groupe de travail ont été intégrés à cette architecture afin de mettre en lumière les lacunes et les chevauchements potentiels. Le groupe a ensuite examiné chacun des enjeux et soumis au Collectif ses commentaires et ses recommandations, qui sont présentés plus loin. L'information est regroupée selon les lacunes et divers autres sous-critères. Le groupe a tâché de s'en tenir à des considérations générales, mais il demeure possible que certains éléments ne concernent que le secteur de la santé.

Afin de faciliter la compréhension des lacunes et la mise en œuvre des recommandations, chaque enjeu est accompagné d'une brève description de sa pertinence pour le cas d'usage des données sur la santé communautaire.

CONSTATS GÉNÉRAUX

Il est important d'uniformiser le vocabulaire entourant les différents enjeux. Ainsi, le Collectif devrait s'assurer de toujours employer les mêmes termes pour éviter la confusion et simplifier la diffusion des normes.

Termes à inclure dans le lexique :

- Rôles (p. ex. propriétaire, consignataire, utilisateur et intendant de données)
- Perspectives (p. ex. fournisseur de données, intermédiaire et consommateur)

Les rôles et les perspectives concernés par chaque norme devront être explicités clairement au cours du processus d'élaboration.

Recommandation : Le Collectif devrait créer un lexique des termes qu'il utilise (et l'harmoniser avec la terminologie employée ailleurs dans les normes) pour assurer l'uniformité des interprétations et de l'application.

À l'aide d'une approche verticale de la gouvernance des données, le groupe de travail a pu cerner plusieurs lacunes potentielles.

- **Objectif général, financement et évaluation :** Toute bonne structure de gouvernance des données doit avoir un objectif clair, un modèle de financement et un programme de travail bien établi. Son efficacité doit aussi faire l'objet de suivis et d'évaluations. Il pourrait exister des normes sur les méthodes d'évaluation.

  Pertinence pour la santé communautaire : La santé est gérée par de multiples organismes indépendants dont la coopération est essentielle. Cependant, les activités de coordination requièrent du financement, et en l'absence de directives et de fonds, les organismes travailleront chacun de leur côté, affaiblissant souvent la chaîne d'approvisionnement des données dans son ensemble.

- **Suivis, vérifications et conformité :** Tout programme de gouvernance des données doit être encadré de suivis, de vérifications et de contrôles de la conformité, dont les résultats sont soumis à un organe exécutif de surveillance.

  Pertinence pour la santé communautaire : De la même façon qu'il faut un objectif commun, il est important de vérifier la conformité à différents points de la chaîne d'approvisionnement des données pour renforcer le lien de confiance entre les acteurs du système et avec les intervenants.

- **Gestion des données autochtones :** Il existe des critères spécialisés pour la gestion des données autochtones (p. ex. principes de PCAP des Premières Nations), qui pourraient aussi être appliqués à d'autres groupes ethnoculturels.

  Pertinence pour la santé communautaire : L'utilisation impropre des renseignements médicaux personnels est l'une des façons les plus manifestes dont les populations autochtones ont été touchées. L'adoption de principes clairs respectant les données autochtones est primordiale pour la réconciliation.

- **Gestion des intervenants :** De nombreux groupes contribuent au cycle de vie des données, et tous devraient être consultés dans la conception et l'administration des systèmes de collecte, de stockage et d'utilisation.

  Pertinence pour la santé communautaire : Comme pour les données autochtones, le public s'inquiète de l'utilisation qui est faite des renseignements médicaux personnels. Ainsi, il sera crucial de comprendre la nécessité de concevoir une chaîne d'approvisionnement des données fiable et de collaborer avec les intervenants pour démontrer cette fiabilité.

- **Souveraineté des données :** Les lois et les lignes directrices encadrant les données au Canada (et dans les provinces et territoires) ne sont pas uniformes. Il en va de même pour les lois sur les données stockées ou envoyées dans d'autres pays. Ce point est particulièrement important pour la propriété intellectuelle (PI) étrangère générée à partir de données canadiennes et la compréhension des droits collectifs.

  Pertinence pour la santé communautaire : Selon les projections, le secteur de la santé devrait connaître une croissance majeure dans les prochaines décennies, d'où la nécessité d'encadrer la création et la protection de la PI. De plus, la protection des données de santé canadiennes envoyées à l'étranger aurait des retombées positives pour tout le pays.

- **Anonymisation des données et réidentification :** L'anonymisation des données – avec des protocoles pour une potentielle réidentification ultérieure – est l'une des meilleures façons de réduire les risques associés aux échanges d'information. Un groupe comme le Canadian Anonymization Network (CANON) pourrait contribuer à l'établissement de normes en ce sens.

  Pertinence pour la santé communautaire : L'utilisation de renseignements médicaux personnels permettant d'identifier les patients comporte un risque important. Il faut donc trouver à modifier les données de sorte à assurer la confidentialité, sans toutefois éliminer d'éléments nécessaires à une analyse efficace. C'est ce à quoi sert l'anonymisation. À noter qu'il est parfois nécessaire de procéder à une réidentification pour des questions de santé individuelle ou publique.

- **Retrait et portée du consentement :** Nous avons besoin de directives claires sur la façon dont les propriétaires de données peuvent retirer leur consentement à l'échelle locale et à différents points de la chaîne d'approvisionnement (parcours) des données.

  Pertinence pour la santé communautaire : Les données médicales passent par plusieurs organismes de soins et de santé publique, et il est essentiel de comprendre comment le consentement fonctionne (et où il est nécessaire) tout au long de son cycle de vie et à tous les points de la chaîne qui le requièrent. La mise en place d'un système de consentement personnel généralisé pourrait par exemple créer un biais statistique.

- **Préservation de la sécurité :** Une chaîne d'approvisionnement des données n'étant aussi solide que son maillon le plus faible, il faudrait s'assurer que tous les partenaires du système emploient des pratiques de sécurité (et de confidentialité).

  Pertinence pour la santé communautaire : Puisque les données médicales passent par plusieurs organismes, les normes de sécurité varient souvent selon le contexte et les objectifs de chacun et le type de données.

- **Technologies infonuagiques :** Étant donné la multiplication des technologies infonuagiques, il pourrait y avoir lieu d'établir des normes sur le stockage de données dans un nuage, particulièrement en ce qui a trait aux droits et aux responsabilités des organismes.

  Pertinence pour la santé communautaire : En santé comme dans la plupart des autres secteurs, les solutions infonuagiques (publiques et privées) sont de plus en plus utilisées. Or, plus les nuages contiennent de données, plus le risque de réidentification augmente.

- **Contrats des fournisseurs :** Les organismes font souvent affaire avec des entreprises de technologie pour coordonner leurs activités et faciliter les échanges de données à l'interne ou avec des partenaires. Cependant, bon nombre des contrats ne tiennent pas compte de la chaîne d'approvisionnement des données dans son ensemble, et il pourrait être pertinent d'établir des pratiques exemplaires et des normes applicables à grande échelle.

  Pertinence pour la santé communautaire : La majorité des technologies utilisées dans le domaine de la santé sont achetées à un fournisseur tiers et non faites sur mesure. Mais comme les contrats des fournisseurs sont souvent négociés par des acteurs qui ne connaissent pas bien le sujet (p. ex. fournisseurs de soins uniques), ils ne servent pas toujours pleinement les intérêts des systèmes de santé. L'adoption de normes assurant la libre circulation des données serait ici bénéfique. Cette recommandation s'inscrit dans les principes du Règlement général sur la protection des données (droit de transfert).

- **Protocoles d'interface de programmation (API) ouverte :** Il pourrait être utile d'établir des normes relatives aux API ouvertes (p. ex. FHIR de HL7 pour les données de santé) pour faciliter les échanges de données entre les différents organismes de la chaîne d'approvisionnement.

  Pertinence pour la santé communautaire : Comme pour le point précédent, le fait de normaliser les protocoles de transfert des données simplifierait le travail des entreprises de technologie et des innovateurs qui utilisent les données de santé, augmentant par la même occasion la valeur de ces données pour les Canadiens. Plusieurs autres pays ont déjà adopté cette approche (notamment le Royaume-Uni et les États-Unis), appliquant des normes comme FHIR de HL7 et SNOMED.

- **Gestion et intendance des normes sur le contenu des données :** Les processus encadrant la gestion des normes sur le contenu des données à différents points de leur cycle de vie sont mal définis et communiqués, surtout lorsque la chaîne d'approvisionnement des données comprend plusieurs organismes. Des groupes comme l'Institute of Electrical and Electronics Engineers (IEEE) ou l'Organisation internationale de normalisation (ISO) pourraient orienter la gestion, la diffusion et la révision des normes.

  Pertinence pour la santé communautaire : Les données de santé ont une grande portée, mais peu de normes universelles les régissent au Canada. Le fait de définir clairement les processus de création, de diffusion et de gestion des normes permettrait de clarifier les obligations redditionnelles.

- **Directives sur les jeux de données minimaux et les éléments de données centraux :** Bon nombre d'organismes emploient des normes axées sur un jeu de données minimal ou des éléments de données centraux, qui, lorsqu'appliquées, facilitent l'échange et la bonne utilisation des données.

  Pertinence pour la santé communautaire : Comme pour le point précédent, le fait de clarifier les processus de création, de diffusion et de gestion des jeux de données minimaux permettrait de préciser les obligations redditionnelles actuelles et d'encourager la définition des lacunes à combler.

- **Utilisation de formulaires et de données non structurées :** Certaines données pourtant très importantes sont collectées de façon non structurée. Il pourrait être utile d'établir un cadre pour trouver un équilibre entre les formulaires et les données non structurées, surtout lorsque des outils d'apprentissage machine sont utilisés.

  Pertinence pour la santé communautaire : Les données de santé ont une grande portée, et si elles sont pour la plupart structurées, ce n'est pas le cas des notes des médecins, qui contiennent des informations précieuses, mais sont parfois difficiles à déchiffrer. L'élaboration de directives et de normes claires sur la façon de combiner formulaires et données non structurées permettrait d'harmoniser les flux de travail cliniques et de se rapprocher des résultats espérés.

- **Gestion des données maîtres :** Bien que la majorité des normes sur le contenu des données se rattachent à un domaine précis, la notion de gestion des données maîtres et la capacité à relier entre eux des jeux de données sont essentielles, surtout dans la chaîne d'approvisionnement des données.

  Pertinence pour la santé communautaire : Pour tirer le meilleur parti des analyses de santé, il faut parfois combiner plusieurs jeux de données. Cependant, ce processus n'est souvent possible que là où des données maîtres uniformes sont employées à grande échelle (sur le plan physique ou logique). En outre, certaines données maîtres s'accompagnent de données connexes qui permettent l'utilisation répétée d'une même donnée collectée une seule fois (p. ex. l'adresse ou l'ethnie).

- **Code de conduite pour les analyses :** En plus du code de conduite éthique, il pourrait être utile de préparer une liste de contrôle normalisée pour la réalisation et la diffusion d'analyses; cela permettrait d'établir la fiabilité des résultats.

  Pertinence pour la santé communautaire : Les solutions d'analyses sont de plus en plus utilisées en santé, mais la multiplication des acteurs pouvant en réaliser fait aussi augmenter les risques d'utilisation impropre des données. La définition d'un code de conduite commun contribuerait à susciter la confiance chez les décideurs et le public.

Recommandation : Le Collectif devrait examiner ces constats et déterminer s'il y a lieu de les ajouter à un enjeu existant ou de créer un nouvel enjeu.

REGROUPEMENTS ET PRÉCISIONS

En transposant les enjeux soulevés par l'ensemble des groupes de travail dans le contexte de ce cas d'usage, le groupe a déterminé que certains points communs permettaient des regroupements. Ce processus a aussi permis de préciser certains des enjeux de sorte à faciliter l'analyse des normes.

Les constats de la présente section sont regroupés par enjeu. L'enjeu principal, en gras, réunit plusieurs sous-enjeux, accompagnés d'une justification et de propositions pour le secteur de la santé communautaire.

Enjeu 1 – Cadre de responsabilité : Cet enjeu devrait comprendre trois volets :

a. Propriétaires de données (obtention, transfert et retrait du consentement)

b. Structures internes des organismes (qui fait quoi)

c. Structures interorganismes (dans une chaîne d'approvisionnement des données)

- **Justification :** Le système de santé est une chaîne d'approvisionnement des données, et la responsabilité doit être examinée à la fois à l'échelle locale, dans le contexte des interactions descendantes et ascendantes avec les partenaires, et sous l'optique du flux de données général et des résultats espérés.
- L'enjeu 5 – Gouvernance de la gestion des données pourrait être intégré au volet b ci-haut :
  a. Intégration de la législation locale et de la Loi sur la protection des renseignements personnels et les documents électroniques
  b. Possibilité d'harmonisation avec la Charte canadienne du numérique
- L'enjeu 24 – Fiabilité des intermédiaires du traitement des données pourrait être intégré au volet b ci-haut :
  a. Définition des intermédiaires en tant que type d'organisation de traitement des données
- L'enjeu 8 – Données ouvertes et procédures d'harmonisation et d'interopérabilité des données pourrait être intégré au volet b ci-haut :
  a. Définition des responsabilités dans les politiques sur les données

Enjeu 30 – Éléments techniques des solutions d'IA : L'ISO travaille actuellement à établir une norme connexe.

- Ce point devrait davantage porter sur la génération d'algorithmes que sur les rapports produits et utilisés (enjeu 33 – Interprétabilité et clarté des systèmes d'IA).
- **Justification :** Les analyses – et surtout l'intelligence artificielle (IA) – sont de plus en plus utilisées en santé. Les solutions d'IA peuvent aussi produire des rapports, mais leurs algorithmes demeurent les principaux livrables de valeur. En effet, ceux-ci peuvent être intégrés aux solutions décentralisées pour faciliter la pose de diagnostics ou servir de base à l'élaboration de politiques fondées sur des preuves.
- Certains points de l'enjeu 35 – Systèmes de gestion de la performance des outils d'analyse et des systèmes d'IA pourraient être déplacés ici.
- Certains points de l'enjeu 33 – Interprétabilité et clarté des systèmes d'IA pourraient être déplacés ici.

Enjeu 2 – Attestations encadrant les rôles professionnels : Cette norme devrait régir le processus d'attestation et non l'attestation elle-même. Des organismes comme ARMA pourraient orienter le travail en ce sens.

- **Justification :** Au Canada, il existe déjà plusieurs organismes qui fournissent des attestations pour l'utilisation des données (p. ex. l'Association canadienne interprofessionnelle du dossier de santé et Digital Health Canada), et leur nombre pourrait bien continuer de croître. Ainsi, il pourrait être utile d'établir des critères pour ces attestations, possiblement à partir des modèles existants.
- L'enjeu 3 – Habileté numérique pourrait être combiné à l'enjeu 2 – Attestations encadrant les rôles professionnels, selon les groupes qu'il concerne. On pourrait ici se pencher sur le degré de connaissance et d'habileté aux différents échelons des organismes.

Enjeu 20 – Accès aux données : La formulation devrait prévoir un accès aux données proportionnel aux besoins.

- **Justification :** La confidentialité est souvent vue comme un obstacle à l'accès aux données de santé, car les responsables de la protection de la vie privée ont une faible tolérance au risque. L'adoption d'approches plus nuancées axées sur les considérations éthiques serait préférable; c'est l'un des points que revendique Statistique Canada dans sa Stratégie des données.
- L'enjeu 22 – Gestion de l'identité : validation et authentification et l'enjeu 25 – Autorisation à la collecte et au partage de données pourraient être combinés à l'enjeu 20 – Accès aux données afin de rassembler toutes les étapes du processus d'accès.

Enjeu 11 – Collecte des données : Plusieurs enjeux différents se rapportent collectivement à la gestion du cycle de vie des données au sein d'un organisme et pourraient donc être regroupés.

- À noter que certains aspects de la collecte de données ont déjà été abordés plus haut (p. ex. les lacunes relatives aux formulaires et aux contrats de fournisseurs).
- On pourrait aussi intégrer des renseignements supplémentaires sur les éléments suivants :
  a. Extraction des données (conservation; enjeu 21)
  b. Portabilité des données (enjeu 29)
- **Justification** : De nouveaux canaux de génération et de collecte des données seront appelés à faire leur apparition; il faudra les intégrer à la chaîne d'approvisionnement des données actuelle.
- L'enjeu 21 – Conservation des données pourrait être intégré aux questions d'extraction des données, ou laissé tel quel.
- L'enjeu 23 – Partage, échange et intégration de données pourrait être ajouté au regroupement ou combiné à l'enjeu 29 – Portabilité et mobilité des données.
- L'enjeu 12 – Gestion des systèmes de données pourrait être ajouté au regroupement.
- L'enjeu 29 – Portabilité et mobilité des données pourrait être ajouté au regroupement ou combiné à l'enjeu 23 – Partage, échange et intégration de données.

Enjeu 6 – Protection des renseignements personnels : La description actuelle vise surtout la propriété des données et les droits, mais il pourrait être plus avisé de mettre l'accent sur la confidentialité des données, notamment sur les évaluations des facteurs relatifs à la vie privée, les ententes de partage des données et la formation du personnel.

- **Justification :** La confidentialité des renseignements médicaux personnels est critique et fait l'objet de mesures législatives partout au pays. Cet enjeu s'étend bien au-delà de la propriété des données et des droits relatifs à l'utilisation des renseignements dans divers contextes et sous diverses formes. Bien que le concept de la confidentialité programmée fasse déjà l'objet d'une norme, il y aurait moyen de le renforcer, comme l'ont fait d'autres pays (p. ex. les principes Caldicott au Royaume-Uni).

Enjeu 31 – Chaînes de valeur des données : Il semble manquer de contenu pour établir une norme. Il faudrait mettre l'accent sur la propriété intellectuelle et le partage de la valeur avec le propriétaire initial des données (p. ex. aux Pays-Bas, les gouvernements envoient leurs données aux entreprises pharmaceutiques, qui en échange financent une partie du système de santé).

- **Justification :** Le système de santé dépend du bon fonctionnement des chaînes d'approvisionnement des données. Les utilisateurs finaux qui génèrent une valeur grâce à ces données (sous forme de PI) pourraient avoir une certaine obligation de la partager avec le reste de la chaîne.

Enjeu 26 – Transparence et communication des analyses de données : L'enjeu 26 pourrait être divisé en deux volets :

a. Éthique, transparence et communication : propriétaires de données

b. Éthique, transparence et communication : utilisateurs des analyses

- L'enjeu actuel vise principalement le volet a, mais le volet b comporte aussi des risques.
- Les travaux d'Edward Tufte discutent abondamment des risques associés au manque d'exigences redditionnelles dans les analyses. Il pourrait y avoir lieu d'établir un code d'éthique à ce sujet.
- Le risque d'enrichissement (couplage) des données fait aussi augmenter le risque de réidentification. Il pourrait être intéressant d'explorer les techniques émergentes comme le chiffrement homomorphique.
- Plus particulièrement, il pourrait être bénéfique d'établir des normes sur la transparence des communications, afin d'éviter que des analyses différentes, mais au premier abord identiques soient comparées (p. ex. le nombre de résultats positifs au test de dépistage de la COVID-19, mesurés différemment d'une région du pays à l'autre).
- Il vaudrait peut-être la peine d'examiner les normes sur les fiducies, les collectifs et les mises en commun de données.
- **Justification :** La transparence sera essentielle pour renforcer la confiance des intervenants dans les analyses de santé qui continuent de se multiplier. Le domaine de la santé est particulièrement nuancé, car l'utilisation des renseignements médicaux personnels dans les analyses a le potentiel de porter atteinte aux patients, surtout lorsque ces derniers font partie de groupes marginalisés (p. ex. hausse considérable des coûts d'assurance pour les personnes souffrant de conditions génétiques préexistantes).

Enjeu 13 – Visibilité des données : Il faudrait limiter cet enjeu aux catalogues et aux recensements de données pour éviter les chevauchements avec l'enjeu 20 – Accès aux données.

- Les énoncés pourraient porter sur la qualité, l'intégrité et la traçabilité des données, mais pas sur les façons d'assurer la qualité (enjeu 18 – Qualité et aptitude à l'emploi des données).
- **Justification :** Les données médicales ont une grande portée, et les points de collecte et d'agrégation sont nombreux. Ainsi, il est difficile pour les organismes de santé de savoir qui détient quelles données et pour combien de temps. Une meilleure visibilité des données – et une meilleure compréhension de leur aptitude à l'emploi – procurerait des gains de rapidité et de confiance.
- Ce regroupement permettrait de traiter plusieurs autres points connexes.
- L'enjeu 16 – Gestion des métadonnées pourrait être ajouté au regroupement.
- L'enjeu 28 – Transparence, parcours et traçabilité des données serait ajouté au regroupement.
- L'enjeu 15 – Marquage manuel des données serait ajouté au regroupement.

Enjeu 18 – Qualité et aptitude à l'emploi des données : Ce regroupement devrait réunir tous les éléments déterminant la qualité des données en un même énoncé sur l'aptitude à l'emploi des données.

- La qualité des données ne peut généralement être évaluée qu'au point d'origine; les autres contrôles visent davantage à mesurer la conformité des données aux modèles autorisés.
- Il pourrait être utile d'élargir la définition de la qualité des données pour englober tous les types de renseignements (qualité de l'information) et ainsi mieux représenter la qualité des études des données. Les lignes directrices sur la qualité de Statistique Canada pourraient être un bon point de départ.
- **Justification :** Compte tenu de la portée et de la complexité considérables des flux de données dans la chaîne d'approvisionnement en santé, il serait important d'évaluer l'aptitude à l'emploi des données utilisées dans les analyses en cherchant un équilibre entre la qualité de ces données et l'utilité des résultats obtenus.
- L'enjeu 18 – Qualité et aptitude à l'emploi des données serait ajouté au regroupement.

Enjeu 33 – Interprétabilité et clarté des systèmes d'IA : Les éléments les plus importants seraient ici l'application des algorithmes d'IA et l'utilisation des études de données.

- La définition pourrait être élargie pour illustrer le caractère explicable des algorithmes statistiques (y compris de l'IA); tous les algorithmes ne sont pas le produit de l'IA, mais ils devraient tous être explicables.
- **Justification :** Plus les solutions d'analyse et d'IA seront utilisées en santé, plus il sera essentiel de pouvoir faire confiance à leurs résultats. Pour établir cette confiance, il faudra d'abord savoir expliquer le fonctionnement des algorithmes.
- L'enjeu 35 – Systèmes de gestion de la performance des outils d'analyse et des systèmes d'IA devrait être ajouté au regroupement.

Enjeu 9 – Rôles des acteurs et des opérations en matière de traitement des données : Cet élément devrait être remplacé par le lexique mentionné plus haut plutôt que de faire l'objet d'une norme.

- **Justification :** La chaîne d'approvisionnement des données comporte plusieurs rôles qui devraient être définis dans un préambule, puis repris dans toutes les normes.

Enjeu 34 – Évaluation et gestion des biais : Cet enjeu pourrait être abordé en même temps que la liste de contrôle pour les analyses mentionnée plus haut.

- Les biais sont autant une question de transparence qu'une question de prise de conscience. Il pourrait être utile d'avoir un système pour traiter les biais inconscients.
- **Justification :** Compte tenu de leur grande portée, les données de santé sont particulièrement vulnérables aux biais intrinsèques introduits par d'anciennes normes. Pour assurer la fiabilité des données, il faudra établir des normes visant la détection et la correction des biais.

Enjeu 17 – Politiques sur les données : gestion des risques et stratégies dans les organisations : Cet enjeu en recoupe beaucoup d'autres (p. ex. l'enjeu 20 – Accès aux données, l'enjeu 6 – Protection des renseignements personnels, et l'enjeu 32 – Transparence et communication des analyses de données).

- Ces différents enjeux pourraient tous être rassemblés dans un même programme de gestion des risques permettant d'optimiser les résultats tout en atténuant le plus possible les effets négatifs.
- **Justification :** La mise en commun des données de santé pour générer des résultats collectifs est un grand travail de coordination qui requiert l'unification des politiques de nombreux organismes. Nous pourrions faciliter cette coordination à l'aide d'une approche commune de gestion des risques traitant de confidentialité, d'accès et d'éthique.

Enjeu 27 – Gestion des ontologies : La définition pourrait être élargie de sorte à fixer des normes explicites pour les données maîtres et la gestion des hiérarchies de données.

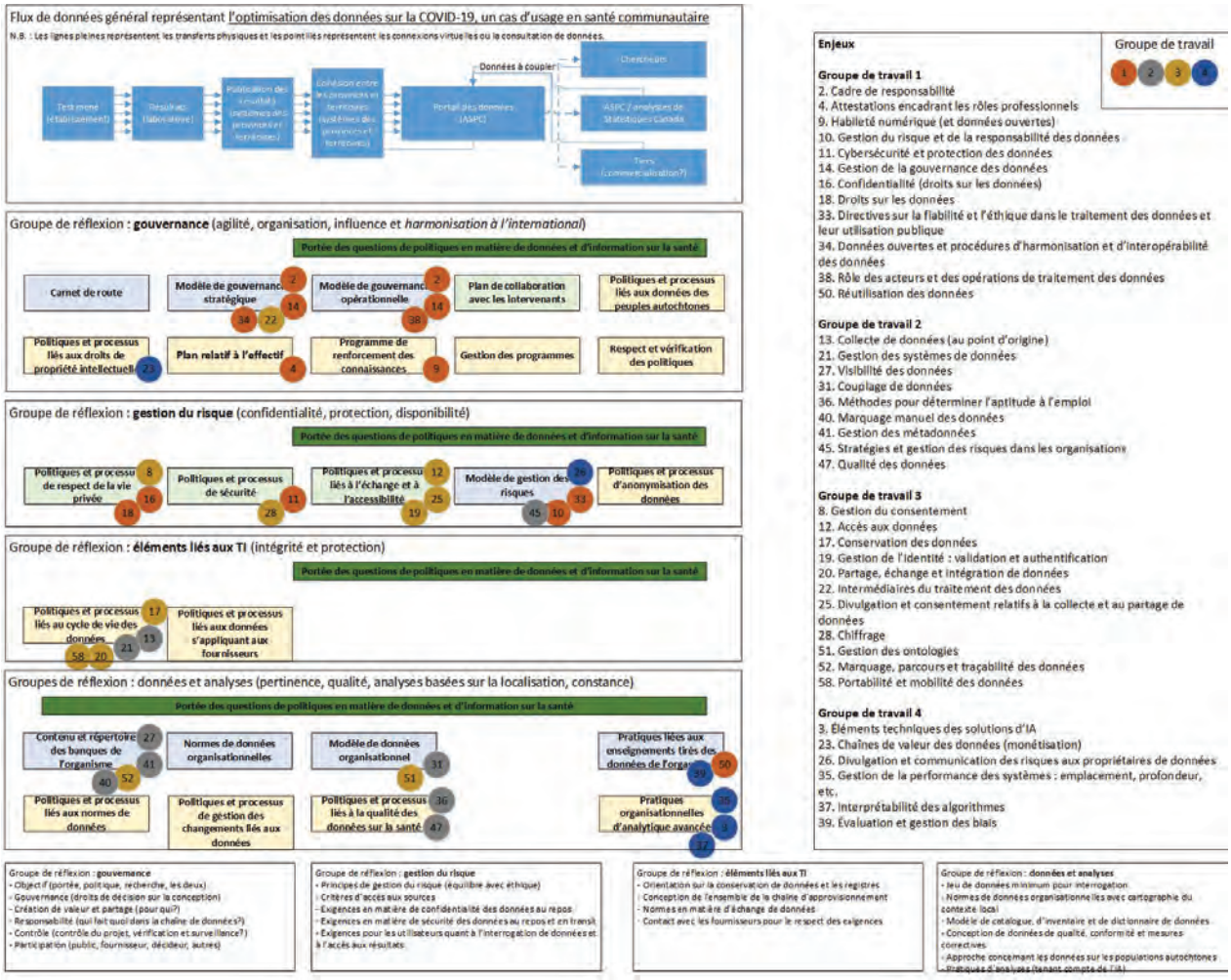
- **Justification :** Les données de santé ayant une grande portée, il serait important de définir des ontologies communes pour faciliter la circulation des données dans la chaîne d'approvisionnement et encourager le couplage de données pour générer de la valeur et des résultats. Nous pourrions nous inspirer de l'European Health Data & Evidence Network et de son utilisation du programme Observational Health Data Sciences and Informatics (OHDSI).
- L'enjeu 14 – Couplage des informations serait ajouté au regroupement.

Recommandation : Le Collectif devrait examiner ces constats et déterminer s'il y a lieu de les ajouter à un enjeu existant ou de créer un nouvel enjeu.

OBSERVATIONS FINALES

La diversité et l'hétérogénéité du système de soins de santé compliquent la normalisation. Cependant, si cette dernière peut aider à protéger les renseignements des individus et améliorer l'efficacité de la gestion des données, il ne faut pas oublier que les données de santé sont régies par un cadre réglementaire complexe, ce qui rend plus difficile l'exploration des innovations en matière de flux de données.

Le groupe de travail est reconnaissant d'avoir pu participer à cette étude de cas. Il s'est inspiré des commentaires recueillis lors des consultations publiques pour formuler les recommandations qu'il soumet à l'examen du Collectif.



Cas d'usage n° 2 – Identité numérique et système bancaire ouvert

Contexte

À l'ère de la COVID-19, où les interactions en personne sont limitées, le travail en contexte numérique gagne en importance pour la population canadienne. Le système bancaire ouvert (ou les finances axées sur les clients) nous en fournit un excellent exemple. La connectivité numérique, les données et les besoins des consommateurs incitent les institutions, les gouvernements et la population à conclure des ententes avec des tiers. Toutefois, en l'absence de réglementation et de normes encadrant ce nouveau secteur, ainsi que d'outils adaptés comme l'identification numérique, la population est laissée pour compte sur les plans économique, concurrentiel, et plus important encore, en matière de sécurité.

Plébiscitée par plus de 70 % de la population canadienne, la collaboration entre secteurs public et privé est essentielle pour instaurer un cadre commun pour l'identité numérique.

Diverses initiatives nationales ont été lancées ces deux dernières années pour appuyer l'identité numérique, le système bancaire ouvert et la normalisation. En 2018, par exemple, le Canada a rejoint un réseau de pays cherchant à mettre les technologies numériques au service des citoyens et dont l'un des pans stratégiques consiste à créer une plateforme d'identité numérique fiable[27]. Le Comité sénatorial des banques et du commerce a également déterminé que le système bancaire ouvert était l'un des principaux cas d'usage sur lequel le Collectif devait se pencher[28]. En 2019, le ministère des Finances a nommé un comité consultatif pour examiner le bien-fondé du système bancaire ouvert qui soulignait notamment l'importance, pour les consommateurs, les entreprises et les entités gouvernementales, de travailler ensemble à l'atteinte d'un objectif commun : créer un écosystème sûr, sécuritaire et digne de confiance pour l'identité numérique canadienne[29]. Il faut en faire une priorité absolue pour les décideurs, les politiciens et les chefs d'entreprise, afin que l'administration publique se donne une politique sur l'identification numérique, que le libellé de cette politique prévoie une identification numérique fiable et que les entreprises soient incitées à explorer des solutions numériques. L'instauration d'un cadre commun pour l'identité numérique passe par la collaboration entre secteurs public et privé, plébiscitée par plus de 70 % de la population canadienne. Notons d'ailleurs que 83 % de la population fait confiance aux administrations publiques et 81 % aux institutions financières pour protéger ses données[30].

IDENTIFICATION NUMÉRIQUE, SYSTÈME BANCAIRE OUVERT ET NORMALISATION

Dans certains pays, l'identité numérique assure la jonction entre partage de données financières, solutions financières innovantes et sécurité. C'est ce que l'on observe en Australie qui, dans le cadre d'un plan de relance économique post-COVID-19, a récemment annoncé un investissement de 256,6 millions de dollars australiens (environ 243 millions de dollars canadiens) destiné à un système d'identité numérique[31]. Malheureusement, le Canada est à la traîne. Bien que le ministère des Finances ait tenu en 2019 une consultation sur les « mérites d'un système bancaire ouvert », parallèlement au lancement de la Charte canadienne du numérique, nous accusons toujours du retard lorsqu'il s'agit de faire le lien entre nos pièces d'identité délivrées par le gouvernement et nos identifiants numériques, volet nécessaire à un encadrement sécuritaire et pratique du système bancaire ouvert. Selon une étude de McKinsey, l'identification numérique complète pourrait dégager des sommes équivalant à 3 à 6 % du PIB en 2030 (en moyenne)[32], soit d'environ 48 à 97 milliards de dollars canadiens.

27 Susan Crutchlow, TransUnion. « Digital Identity – A Key Driver of Canada's Digital Economy ». https://www.transunion.ca/blog/digital-identity.
28 Rapport du Comité sénatorial permanent des banques et du commerce. *Un système bancaire ouvert, qu'est-ce que cela signifie?* https://www.sencanada.ca/fr/info-page/parl-42-1/banc-systeme-bancaire-ouvert/.
29 CCIAN. « L'impact économique de l'identité numérique au Canada ». https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.
30 CCIAN. « Les Canadiens sont prêts à adopter l'identité numérique ». https://diacc.ca/fr/2019/10/15/les-canadiens-sont-prets-a-adopter-lidentite-numerique/.
31 Premier ministre de l'Australie. *Digital Business Plan to Drive Australia's Economic Recovery*. https://www.pm.gov.au/media/digital-business-plan-drive-australias-economic-recovery.
32 McKinsey Global Institute. Digital Identification : A Key to Inclusive Growth. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

Les gouvernements, les institutions financières et les entreprises de technologie financière utilisent déjà une forme d'identification numérique (c.-à-d., accès à Service Canada ou à l'Agence du revenu du Canada, production de déclarations de revenus en ligne ou services bancaires en ligne). Toutefois, en l'absence d'un cadre canadien de gestion de l'identité appuyé par une normalisation et une réglementation robustes, le fonctionnement actuel de l'identification numérique au Canada présente des défis. Les identités en ligne sont fragmentées entre de nombreuses entreprises et entités, ce qui accroît le risque systémique de fraude par accumulation de données. Résultat : des atteintes à la sécurité des données qui minent la confiance des gens envers les organisations touchées et l'économie numérique[33]. Traditionnellement, l'identité se prouvait au moyen de documents physiques (passeports, cartes d'identité, etc.). Or ces documents physiques peuvent être contrefaits ou modifiés, et la fraude entraîne des pertes financières importantes. De plus, bon nombre de personnes n'ont pas les moyens de prouver leur identité, ce qui les empêche d'accéder facilement à des services numériques, comme les soins de santé, les services gouvernementaux et les services bancaires. En cette période difficile, cette situation est plus que jamais d'actualité.

La population canadienne souhaite un meilleur contrôle et un accès plus souple à ses données, ce qui est logique sur le plan économique. Pendant ce temps, des millions de Canadiens et de Canadiennes partagent déjà des renseignements bancaires avec des fournisseurs tiers. L'absence d'une formalisation du système bancaire ouvert les contraint toutefois à recourir à des méthodes peu sécuritaires telles que la capture d'écran, qui mettent en danger la confidentialité de leurs données personnelles et financières. Un cadre d'identité numérique canadien présente un potentiel d'économies nettes par établissement de 100 millions de dollars canadiens ou plus par année, grâce à l'efficacité opérationnelle… et à la prévention de la fraude[34]. Compte tenu de ces défis, la normalisation est une solution possible pour mettre en œuvre un cadre d'identité numérique canadien qui reflète les valeurs défendues par la population canadienne (inclusion, transparence et confiance).

Séances de discussion sur l'identité numérique et le système bancaire ouvert

Les 2, 3 et 4 décembre 2020, le CCN et le Collectif ont consulté la population sur les thèmes de l'identité numérique et du système bancaire ouvert en organisant des séances de discussion – deux en anglais et une en français. Ces séances ont attiré plus de 100 participants de partout au pays, dont des représentants d'institutions financières et de fournisseurs de services tiers.

Chaque séance a commencé par un bref exposé des représentants du CCN sur le rôle du Collectif et l'importance des normes, suivi d'un état des lieux de l'identité numérique et du système bancaire ouvert au Canada. Les participants ont ensuite été invités à s'exprimer sur deux grands thèmes :

- l'état actuel de l'identité numérique et du système bancaire ouvert au Canada, notamment les possibilités et les défis actuels ainsi que les règles et les normes existantes;
- l'avenir idéal dans ces deux domaines : avantages souhaités pour les consommateurs, et lois et règlements nécessaires à une structuration efficace de l'identité numérique et du système bancaire ouvert.

ÉTAT DES LIEUX ET DÉFIS ACTUELS

Pour lancer la discussion, une activité a été organisée autour d'un tableau blanc interactif pour amener les participants à exposer leurs points de vue sur les défis propres au Canada dans les domaines de l'identité numérique et du système bancaire ouvert. Quatre grands thèmes récurrents sont ressortis de ces discussions :

1. la confiance, plus précisément la nécessité de gagner et de conserver la confiance des consommateurs;
2. la sécurité, ou la nécessité de gérer les risques, de préserver la confidentialité et de prévenir la fraude;
3. la fragmentation, et la nécessité d'optimiser la coopération, l'interopérabilité et l'efficience;
4. une gouvernance et une surveillance efficaces, soit la nécessité d'établir des règles, des règlements et des normes cohérentes et harmonisées d'une province et d'un territoire à l'autre.

33 CCIAN. « L'impact économique de l'identité numérique au Canada ». https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.
34 CCIAN. «Industry Insights: Digital ID in Financial Services». https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.

Après l'activité, les participants ont discuté en petits groupes. En réfléchissant à la situation actuelle de l'identité numérique et du système bancaire ouvert au Canada, la plupart ont estimé que le pays est extrêmement bien placé pour devenir un chef de file dans ces deux domaines. Toutefois, ils ont également convenu que le Canada prend du retard sur d'autres pays en ce qui concerne l'élaboration des cadres juridiques et réglementaires requis. De nombreux participants ont fait remarquer qu'il fallait davantage de leadership et de soutien du gouvernement fédéral dans ces domaines, car il n'existe actuellement aucune loi permettant et encadrant le développement du système bancaire ouvert au Canada. Parmi les autres lacunes évoquées par les participants figure le manque de connaissances des consommateurs canadiens, qui les empêche d'utiliser en toute confiance l'identité numérique et le système bancaire ouvert. Cependant, les participants ont également noté qu'il revient aux administrations publiques et aux acteurs du secteur de faire connaître le système bancaire ouvert et de gagner la confiance des utilisateurs.

AVENIR IDÉAL

Les participants se sont ensuite penchés sur l'avenir souhaité en matière d'identité numérique et de système bancaire ouvert et ont globalement convenu que le consommateur devrait jouir d'un contrôle et d'un pouvoir décisionnel accrus sur l'accès et l'utilisation de ses données personnelles. Selon eux, un tel résultat passe par un changement de paradigme fondamental : une transition de la propriété et du contrôle institutionnels des données à un modèle plus transparent et démocratique, axé sur le consommateur. Ils ont imaginé un système national d'identité numérique complet et fiable fonctionnant de manière transparente à l'échelle nationale et provinciale. Par ailleurs, ils ont souligné que le succès était conditionnel à une utilisation et à une interopérabilité étendues des systèmes ainsi qu'à la mise en place de solides mécanismes de protection de la confidentialité.

DISCUSSIONS

État des lieux de l'identité numérique et du système bancaire ouvert

Au cours de la première partie des discussions en petits groupes, les participants ont été invités à dresser un état des lieux de l'identité numérique et du système bancaire ouvert au Canada.

Les thèmes récurrents et les principales conclusions des discussions sont résumés ci-dessous.

Q1.1 : Quel est le portrait actuel de l'identité numérique et du système bancaire ouvert (c.-à-d. quels renseignements sont requis, quel est le niveau de sécurité associé à ces renseignements et qui y a accès)?

Thème no 1 : Le Canada est bien placé pour encadrer l'identité numérique et le système bancaire ouvert, mais accuse du retard par rapport aux autres pays.

Selon certains participants, le Canada est extrêmement bien placé pour s'adapter aux technologies et solutions numériques émergentes et les exploiter, et pour s'ériger en chef de file des domaines de l'identité numérique et du système bancaire ouvert. Les participants ont souligné que le pays dispose de compétences et de connaissances uniques dont il peut tirer parti, en particulier dans ses secteurs des services financiers et des technologies, de calibre mondial. Un participant a utilisé l'analogie suivante pour expliquer la situation actuelle au Canada : « C'est comme si nous avions des chaussures de sport, mais que nous ne les avions pas encore enfilées. » De nombreux participants ont fait remarquer qu'il faut davantage de leadership et de soutien du gouvernement fédéral dans ces domaines, car il n'existe aucune loi au pays permettant et encadrant le développement du système bancaire ouvert.

Tous les groupes se sont accordés pour dire que, comparativement aux autres pays, le Canada peine à se doter des moyens nécessaires au déploiement de l'identité numérique et du système bancaire ouvert. Les participants ont fait remarquer que de nombreux acteurs étrangers sont très en avance sur le Canada, tant sur les plans technologique que réglementaire. Des territoires et pays comme le Royaume-Uni, l'Australie et Hong Kong ont été cités comme des acteurs clés ayant « des années d'avance » sur le Canada. Une question importante a été posée au cours des séances : « Quelles leçons pouvons-nous tirer du succès des infrastructures étrangères? Nous devons reconnaître l'excellence des autres pays et adopter ou mettre en œuvre les pratiques exemplaires. »

Considérant le facteur temps comme essentiel, certains participants ont suggéré que le Canada devait éviter de s'enliser en « réinventant la roue ». Un participant a déclaré : « Nous sommes tellement en retard. Commençons quelque part. Nous devons trouver un juste équilibre entre l'action et la perfection. »

Plusieurs participants ont fait remarquer que le Canada s'appuie encore sur des systèmes faisant la part belle au papier pour les opérations bancaires et l'identification, et qu'il faut poursuivre la transition vers des solutions numériques. L'un d'entre eux a fait remarquer que pour ouvrir un compte bancaire, il faut se rendre en personne à la banque pour présenter plusieurs documents. Il a reconnu qu'un changement s'opère peu à peu, mais que les règles varient d'une banque à l'autre. Les participants ont affirmé que si nous pouvions normaliser sous forme numérique les documents d'identité comme le passeport ou le permis de conduire, l'interopérabilité s'en trouverait améliorée.

Thème n° 2 : La connaissance et la compréhension des consommateurs à l'égard des concepts d'identité numérique et de système bancaire ouvert sont limitées.

Le manque de sensibilisation et de connaissances de la population sur l'identité numérique et le secteur bancaire ouvert a été souligné. Les participants ont relevé la nécessité d'expliquer les concepts de manière claire et simple pour atteindre un niveau de confiance fondamental au sein du public. En ce qui concerne le partage et la conservation des données, de nombreux participants ont souligné que, pour obtenir la participation des consommateurs canadiens et leur confiance à l'égard des tiers, il faut absolument qu'ils comprennent quelles données seront conservées, pendant combien de temps et dans quel but. Lors d'une des séances de concertation, des participants ont également recommandé d'intensifier les apprentissages liés à la cybersécurité et à l'identité numérique en milieu scolaire.

Les risques liés à la confidentialité et à la sécurité étaient également au centre des préoccupations des participants, d'autant plus que ces risques touchent les personnes et leurs renseignements personnels et bancaires. Les participants ont laissé entendre que l'ouverture d'un compte bancaire s'accompagne parfois d'un partage excessif des renseignements fournis, et ils se préoccupent de l'usage qu'en font les banques. Certains craignent que les consommateurs ne perçoivent pas ces risques.

PROBLÈMES DE NORMALISATION

- La concurrence est un puissant moteur à de nombreux égards – tant que le système bancaire ouvert existe de manière non structurée. Les normes pourraient être utilisées pour renforcer l'emprise des différents acteurs sur le marché, ou pour ériger des obstacles. Le consommateur doit être au premier plan.
- Les modalités de consentement sont trop complexes et techniques pour que le citoyen moyen puisse les comprendre et prendre une décision éclairée lorsqu'il transmet ses données.
- La normalisation suscite une certaine perplexité relative à l'interopérabilité entre les secteurs et sur le plan numérique.
- Le consommateur doit recevoir des explications exprimées dans un langage simple.
- De nos jours, des services sont proposés à la population sans égard à la sécurité. C'est la praticité qui l'emporte. Il faut instaurer des garde-fous.
- Chaque dépositaire d'information peut fixer ses propres normes. Nous devons nous éloigner de l'accès à l'information ou de l'authentification basés sur la connaissance et nous baser sur les principes à respecter pour avancer ensemble plus rapidement. Pour aller de l'avant, il faut donner les moyens d'agir à des dépositaires de confiance.
- En ce qui concerne les normes et politiques, comment atténuer le risque pour certains segments de la société canadienne qui ne peuvent pas ou ne souhaitent pas prendre le virage de l'identité numérique ou des transactions numériques? Comment les normes s'appliqueront-elles à ces segments?

Q1.2 : À votre connaissance, quels sont les règles, règlements ou normes en place pour réglementer l'identité numérique et le système bancaire ouvert?

Thème no 3 : Plusieurs autres pays ont mis en œuvre des règles, mais les approches varient et manquent de cohérence.

Les participants ont mentionné diverses normes mises en œuvre par certains pays. Notant une divergence d'approches, certains participants ont déclaré qu'il serait avantageux d'établir des normes internationales communes (par exemple entre le Canada et le Royaume-Uni) afin de faciliter, entre autres, le commerce et la mobilité à l'échelle internationale.

Voici quelques exemples de normes existantes :

- La transformation numérique des services publics en Estonie en cours depuis plus de dix ans
- L'interface de programmation d'application (API) ouverte de l'Autorité monétaire de Hong Kong pour le secteur bancaire
- Les normes sur le système bancaire ouvert au Royaume-Uni et le passage à la finance décentralisée
- Les initiatives liées au système bancaire ouvert en Australie, en Nouvelle-Zélande et au Mexique selon une approche plus horizontale

Thème no 4 : Il n'existe pas de règles pour garantir le recueil du consentement au partage des données personnelles.

De nombreux participants ont fait remarquer l'insuffisance des normes et règles en place pour garantir que les consommateurs ne partagent que les données strictement nécessaires à l'accès aux services. L'un d'entre eux mentionnait ceci : « Lorsque vous vous rendez au magasin de vins et de spiritueux, vous devez présenter votre carte d'identité pour prouver que vous avez l'âge légal pour boire. Lorsque le caissier demande à voir votre pièce d'identité, généralement votre permis de conduire, il ne voit pas seulement votre âge; il a aussi accès à une myriade d'autres renseignements personnels. » La question du consentement a également été soulevée. Certains participants ont fait remarquer que le consentement devrait précéder tout partage des renseignements personnels.

EXEMPLES DE NORMES EN VIGUEUR

- Cadre de confiance pancanadien (CCP)
- Normes ouvertes pour les API

Avenir de l'identité numérique et du système bancaire ouvert

Dans la seconde partie des discussions en petits groupes, les participants ont été invités à se prononcer sur l'avenir souhaité de l'identité numérique et du système bancaire ouvert au Canada.

Voici les thèmes récurrents et les principales observations qui en sont ressortis.

Q2.1 : Quel est l'avenir idéal de l'identité numérique et du système bancaire ouvert au Canada (c.-à-d. quels sont les cas de figure idéaux, les avantages que présente la montée en puissance de la surveillance en ligne pour les consommateurs et les fournisseurs de services)?

Thème nº 5 : Un changement de paradigme vers un modèle axé sur le consommateur, qui conserve la propriété et le contrôle de ses données.

Parmi les thèmes qui sont revenus comme des leitmotive lors des discussions figure l'idée d'un changement de paradigme : passer de la propriété et du contrôle institutionnels des données à un modèle plus transparent et démocratique, axé sur le consommateur. L'importance de donner à chaque consommateur les moyens et les outils pour contrôler l'accès à ses données personnelles, leur utilisation et leur partage a été soulignée au cours de plusieurs séances. Cet enjeu a soulevé des questions : « Comment pouvons-nous donner le contrôle à l'utilisateur? Comment pouvons-nous le laisser exploiter ses renseignements personnels et les utiliser comme il l'entend? »

Lors d'une séance, des participants ont avancé que le fait de donner aux consommateurs l'accès à leur identité numérique pourrait leur faciliter l'accès à plusieurs comptes bancaires. Ils pourraient ainsi autoriser le partage de données avec les institutions de leur choix et retirer l'autorisation donnée à ces dernières de partager les données entre elles.

En discutant de la transition vers un modèle axé sur le consommateur, les participants ont fait remarquer que la concrétisation d'un tel modèle passerait par l'éducation des consommateurs, qui doivent pouvoir mesurer le contrôle et le pouvoir qu'ils ont sur leurs données et connaître les avantages et les risques associés à l'identité numérique et au système bancaire ouvert. Par exemple, un participant a déclaré qu'en tant que consommateur, il ne sait pas où vont ses données, même s'il prête attention au consentement. « Même lorsque vous payez quelque chose, là encore, vous ne savez pas où vos données sont transmises, ce qui est préoccupant. Cela ne favorise pas la confiance ». Le concept de « consentement éclairé » a été étudié tout au long des séances, et les participants ont conclu qu'il convient d'en préciser et d'en simplifier la définition.

Thème nº 6 : L'interopérabilité est synonyme d'intégration et de valeur ajoutée.

Lors de plusieurs séances, il a été question des avantages et des intérêts de l'interopérabilité, notamment en ce qui concerne l'accès aux données par-delà les systèmes, les compétences provinciales et les frontières internationales. Soulignant les avantages possibles pour les consommateurs, plusieurs participants ont donné l'exemple des personnes vivant et travaillant dans diverses régions canadiennes et d'autres pays qui, grâce à un accès à leur identité numérique ainsi qu'à leurs données personnelles et financières, peuvent obtenir des services localement.

Les participants ont expliqué que l'interopérabilité n'est pas qu'une question de technologie; elle touche également le système de lois, de règlements et de normes internationales. Les protocoles et les règlements doivent permettre à toutes les entités de travailler ensemble.

En outre, les participants ont fait observer qu'une participation étendue est un préalable à l'interopérabilité. Si les principaux acteurs du secteur privé restent sur la touche ou si les obstacles à la participation sont trop importants pour les prestataires de services de petite taille ou spécialisés, l'intérêt et les avantages pour les consommateurs seront limités.

Q2.2 : Quelles règles, réglementations ou normes sont nécessaires à la structuration de l'identité numérique et du système bancaire ouvert au Canada?

Thème nº 7 : Prêter attention à la confidentialité.

Les participants ont fait remarquer que de solides mécanismes de protection de la confidentialité s'imposent pour réduire au maximum le risque que les renseignements personnels soient partagés à outrance, mal gérés ou compromis. L'un d'entre eux a suggéré qu'un système décentralisé pourrait être plus résilient et sécuritaire, car un système centralisé comporte un point de panne unique, et que les données, stockées à un seul endroit, sont plus vulnérables aux attaques et aux fraudes.

Thème nº 8 : Harmonisation et création d'un cadre national de gestion de l'identité numérique.

Les participants ont souligné le besoin d'un système de gestion de l'identité numérique complet qui soit opérationnel à l'échelle nationale et provinciale et qui fournisse une façon claire et simple d'instaurer un lien de confiance avec le public canadien. Il ressort des discussions que l'identité numérique relèvera des gouvernements provinciaux, ce qui pose le problème de la compétence. Il convient donc d'harmoniser les lois et règlements fédéraux et provinciaux pour que le système fonctionne de manière homogène dans tout le pays.

Thème nº 9 : Établir des définitions claires et utiliser une terminologie cohérente.

Les participants estiment que la confusion règne chez les consommateurs sur la nature réelle de l'identité numérique et ses conséquences sur eux. L'identité numérique doit être clairement définie et formulée avant qu'on puisse étudier ses répercussions sur des secteurs comme le milieu bancaire. Les participants ont également fait remarquer qu'il convient de préciser les différences entre les concepts d'identité numérique et de système bancaire ouvert. Par ailleurs, le terme « système bancaire ouvert » a fait débat, certains laissant entendre qu'il véhiculait la notion de laisser-faire ou d'anarchie, lui préférant le terme « finances axées sur les clients ». Ils ont aussi souligné l'importance d'utiliser un langage simple lorsque l'on tente d'éduquer le consommateur, car le jargon ou un vocabulaire technique complexe alimentent la confusion.

Thème nº 10 : Apprendre des autres pays et adopter les pratiques exemplaires internationales.

Comme mentionné précédemment, les participants ont reconnu que d'autres pays sont plus avancés dans la mise en œuvre de l'identité numérique et du système bancaire ouvert. Sur le plan des règles et des normes, ils y voient une occasion de tirer les enseignements de ces diverses expériences et d'adopter au Canada des approches et des pratiques exemplaires éprouvées et fructueuses. Ces pratiques exemplaires peuvent servir à orienter l'élaboration de règlements et de normes efficaces au pays.

À CONSIDÉRER POUR L'ÉLABORATION DE NOUVELLES NORMES

Audit : Activités de certification et d'accréditation visant le maintien des normes pour lesquelles il existe actuellement une différence d'interprétation

- **Opérations :** Exigences pour la normalisation des opérations
- **Partage des données :** Élaboration d'un cadre technique et d'une norme commune pour le partage des données
- **Norme relative à la confiance et à l'identité numériques :** Soumission du marché à des exigences établies par consensus
- **Coopération internationale en matière d'élaboration de normes :** Par exemple, entre le Canada et le Royaume-Uni à l'Open Data Institute
- **Adhésion :** Pour susciter l'adhésion, les normes doivent encourager un modèle de fonctionnement fédérateur sur le plan humain, et protéger et promouvoir le commerce. Sinon, leur adoption en sera retardée.

Rapport du groupe de travail sur le cas d'usage

PRÉFACE

Bien que le secteur privé canadien mette à la disposition de la population des cadres et outils d'authentification, en l'absence de système d'identité numérique et de système bancaire ouvert reconnus à l'échelle nationale, le Canada demeure à la traîne. Ce décalage prive les citoyens de services en ligne et de la possibilité de transmettre en toute sécurité leurs données aux entités de leurs choix. Des systèmes d'authentification désuets sont couramment utilisés : cartes d'identité physiques ou photos de ces cartes, mots de passe et questions de sécurité… Chronophages et complexes, ils posent des risques de fraude et de vol d'identité. Certaines personnes choisissent de se priver de services de gestion financière innovants ou de transmettre leurs données de manière moins sécuritaire.

Pour le Canada, les risques s'articulent autour de trois axes : l'impossibilité pour la population de bénéficier d'un système d'identification en ligne et de transmission des données plus sécuritaire; un progrès technologique débridé qui irait dans plusieurs directions et empêcherait l'interopérabilité du système; et un frein à la compétitivité des innovateurs canadiens qui cherchent à développer leurs idées à l'international. Par son inaction, le pays serait rapidement dépassé par les innovateurs et les fournisseurs de service étrangers.

Le Canada doit donc à tout prix mettre les personnes et le numérique à l'avant-plan pour donner les moyens aux gens de protéger leur vie privée. Par son approche et sa conception de l'identité numérique, notre pays s'érige en chef de file mondial. Le monde a les yeux rivés sur notre approche public-privé en partenariat avec la population. Axée sur la juste répartition des retombées économiques, cette approche centrée sur les Canadiens et les Canadiennes est unique au monde, et c'est ce qui fait qu'elle attire autant l'attention à l'international. Or en ce qui a trait à l'identité numérique nationale, nous sommes à la traîne. Nous avons grandement besoin de volonté politique, d'une réforme innovante des politiques et de l'adoption de technologies fondées sur des normes.

L'identité numérique et le système bancaire ouvert sont des enjeux distincts. Nous aurions pu les considérer individuellement, mais le présent rapport traite des deux enjeux et de leur interdépendance. Il appuie les 35 recommandations de la feuille de route du Collectif, qui situe le Canada en matière de gouvernance des données et énonce les raisons d'être de cette gouvernance. Non prescriptive, la feuille de route vise à décrire le paysage normatif actuel de la gouvernance des données aux intervenants et à rassembler efficacement les bribes de conversation sur ces enjeux complexes et difficiles. Les recommandations, en appui aux diverses initiatives actuelles des gouvernements et des entreprises, visent à cibler les enjeux de gouvernance des données pertinents et à combler les lacunes.

La feuille de route repose sur un consensus entre les personnes et les organisations qui ont activement participé à son élaboration et ne reflète pas nécessairement le point de vue individuel de chacune d'elles.

SYNTHÈSE

Fondé à l'été 2019, le Collectif est un organe de coordination intersectoriel qui a pour but d'accélérer, à l'échelle de l'industrie, l'élaboration de normes et de spécifications qui répondent aux besoins des intervenants et catalysent la croissance des capacités en matière de gouvernance des données en fonction des priorités nationales et mondiales. Il rassemble plus de 220 experts issus de tous les ordres de gouvernement, de groupes autochtones, du milieu de la recherche, du secteur privé, des ONG et d'organismes spécialisés en confidentialité et en éthique d'un océan à l'autre, tous animés par une même mission. Il travaille sur une feuille de route de normes pour une bonne gouvernance des données, afin de définir les besoins de normalisation en se fondant sur plusieurs cas d'usage.

Comme les données sont un actif incorporel, l'importance dans le quotidien de concepts abstraits comme la gouvernance des données et le rôle de la normalisation dans la collecte, le partage et l'utilisation de données n'est pas toujours facile à conceptualiser. Les cas d'usage servent d'exemples pour aider les intervenants à comprendre comment les normes peuvent renforcer la gouvernance des données et la confiance.

Le groupe de travail du Collectif sur le cas d'usage de l'identité numérique et du service bancaire a vu le jour à l'été 2020. Formé d'un petit groupe d'experts, il a discuté des lacunes cernées par le Collectif en lien avec cet enjeu. Le cas d'usage ne visait pas à concevoir une norme ou à proposer des lignes directrices en la matière, mais plutôt à préciser les lacunes afin d'étayer la feuille de route du Collectif, en tenant compte des éléments suivants :

- les exigences en matière de vérification et d'authentification de l'identité – en tenant compte des difficultés éprouvées par certaines personnes à prouver leur identité ou à accéder à des services en ligne;
- le contrôle, l'accès et la confidentialité des données des consommateurs;
- les protocoles de sécurité pour le partage de données sur les clients (normes sur les API)
- les directives opérationnelles sur les risques de la mise en œuvre et de l'adoption;
- les directives relatives à l'expérience de la clientèle reflétant des valeurs d'inclusion, de transparence et de confiance.

Dans le cadre de cinq rencontres et d'une consultation publique, les membres du groupe de travail ont échangé leurs points de vue sur les défis qui attendent l'identité numérique et le système bancaire ouvert au pays. Le groupe de travail a recommandé la prise de mesures immédiates, en s'appuyant sur ce qui avait été fait par le passé, pour éviter que se creuse encore davantage le fossé qui sépare le Canada des autres pays.

De ces échanges, sept recommandations sont ressorties :

1. La mise en œuvre immédiate d'une approche mettant les personnes et le numérique à l'avant-plan pour donner les moyens aux gens de protéger la confidentialité de leurs données sans empêcher leur transmission. Les gens bénéficieraient du droit reconnu de contrôler et de partager leurs données avec les entités de leur choix. L'approche adoptée doit être stratégique, coordonnée et multisectorielle, pour préserver les droits des consommateurs à contrôler et à utiliser leurs données. La collaboration entre les gouvernements et les entreprises visant à mettre en place des cadres réglementaires le plus rapidement possible serait profitable pour la population, et les consommateurs doivent être au centre de ces cadres d'identité numérique et de système bancaire ouvert.
2. La réunion d'un grand groupe d'experts praticiens de la technique et des politiques qui examinerait et recommanderait l'adoption de normes et la mise en œuvre d'activités connexes, existantes ou nouvelles, qui tiennent compte des besoins et des exigences de la population, en s'appuyant sur des travaux existants. Pour ce faire, il faudra évaluer les cadres en place et voir si les efforts de normalisation technologiques actuels peuvent répondre à ces besoins. Des normes comme les Normes nationales du Canada peuvent faire converger divers points de vue en vue d'un travail de normalisation qui repose sur le consensus et inclut les entreprises, les chercheurs, les consommateurs et les gouvernements. Voici les besoins en matière de normalisation :
   - l'accès, la conservation, la gestion, le traitement et le partage de données;
   - les exigences en matière de confidentialité, de sécurité et de transparence;
   - l'interopérabilité entre les provinces et territoires et entre les marchés verticaux;
   - la vérification des identifiants, notamment des niveaux clairs d'assurance pour garantir l'interopérabilité.
3. La mobilisation de l'industrie, des chercheurs, des groupes de consommateurs et de tous les ordres de gouvernement (fédéral, provinciaux et territoriaux) comme partenaires actifs participant à l'élaboration de Normes nationales du Canada, ou d'autres documents normatifs, ainsi qu'aux efforts de normalisation internationaux. Cela passerait entre autres par la collaboration et la coordination avec des organismes internationaux et la promotion active à l'international de l'adoption de normes canadiennes, lorsque c'est pertinent.
4. La mise en œuvre de plans de communication stratégiques et tactiques et des investissements dans la sensibilisation des consommateurs aux droits qu'ils ont sur leurs données et à l'exercice de ces droits. L'identité numérique et le système bancaire ouvert sont complexes : la participation de la population est essentielle pour bâtir des connaissances et instaurer la confiance sur les enjeux de vie privée et de sécurité.
5. La mise en place d'un cadre de confiance central qui permettrait à la population d'accéder à ses données et de les partager en toute sécurité. Un tel cadre balisant l'identité numérique ou le secteur bancaire ouvert devrait s'harmoniser avec les normes et pratiques exemplaires nationales et internationales pertinentes; la législation et la surveillance ne devraient pas freiner l'innovation et l'émergence de cas d'usage. Il serait le fruit de l'adoption, de l'adaptation ou de l'élaboration d'un cadre, nouveau ou existant, ou d'une collaboration public-privé. Le gouvernement y participerait assurément, mais le travail doit se faire en collaboration avec le secteur privé, comme le réclame 66 % de la population[35]. Le tout garantirait l'interopérabilité et s'attaquerait à des enjeux importants comme la confidentialité, la sécurité et les interactions transfrontalières.
6. L'établissement, grâce aux outils de normalisation, des critères d'un cadre d'accréditation permettant aux organisations publiques et privées de créer et de vérifier des identités numériques et d'échanger des données dans un système bancaire ouvert.
7. Le stockage des données sous une forme utilisable et partageable et l'amélioration de protocoles de sécurité allant au-delà des mots de passe et des questions de sécurité (qui peuvent être volés ou piratés), par les entités publiques et privées qui recueillent et utilisent des renseignements personnels afin de donner l'exemple.

Le présent rapport porte sur le cas d'usage sur l'identité numérique et le système bancaire ouvert. Pour les besoins de ce rapport seulement, les définitions suivantes sont utilisées comme convenu par le groupe de travail sur les cas d'usage (d'autres termes et définitions se trouvent à la fin du rapport) :

35 CCIAN 2020. https://diacc.ca/fr/2021/02/16/la-covid-19-a-accelere-la-demande-des-canadiens-pour-une-identite-numerique/.

Identité numérique : Si l'identité est un « ensemble d'indicateurs (ou d'attributs) sur une personne (entité) qui la rendent unique, l'identité numérique est un ensemble d'attributs qui permettent d'associer une entité personnelle à ses interactions virtuelles en utilisant des sources fiables… un peu comme une empreinte en ligne ». Elle correspond également à l'information utilisée par les systèmes informatiques pour reconnaître une personne ou une organisation externe et lui donner un accès sécuritaire et efficace à des services numériques. Elle donne plus de contrôle aux consommateurs sur leurs données et leur identité en leur permettant de choisir l'information à transmettre selon la situation. Elle « peut être normalisée et utilisée entre les entités, et on peut y ajouter de l'information[36] ».

Système bancaire ouvert (finance axée sur les clients) : Cadre de règlements et de normes où « les consommateurs et les entreprises peuvent autoriser des tiers fournisseurs de services financiers à avoir accès aux données sur leurs opérations financières au moyen de canaux sécurisés en ligne[37] ».

À l'ère de la COVID-19, où les interactions en personne sont limitées, le travail en contexte numérique gagne en importance pour la population canadienne. Le système bancaire ouvert (ou les finances axées sur les clients) nous en fournit un excellent exemple. La connectivité numérique, les données et les besoins des consommateurs incitent les institutions, les gouvernements et la population à conclure des ententes avec des tiers. Toutefois, en l'absence de réglementation et de normes pour soutenir ce nouveau secteur ainsi que d'outils adaptés comme l'identification numérique, la population est laissée pour compte sur les plans économique, concurrentiel et, plus important encore, en matière de sécurité.

Diverses initiatives nationales ont été mises sur pied ces deux dernières années pour appuyer l'identité numérique, le système bancaire ouvert et la normalisation. Il est impératif que le Canada s'appuie sur ce qui a déjà été fait. En 2018, par exemple, le Canada a rejoint un réseau de pays cherchant à mettre les technologies numériques au service des citoyens et dont l'un des pans stratégiques consiste à créer une plateforme d'identité numérique fiable[38]. Le Comité sénatorial des banques et du commerce a également déterminé que le système bancaire ouvert était l'un des principaux cas d'utilisation sur lequel le Collectif devait se pencher[39]. En 2019, le ministère des Finances a nommé un comité consultatif pour examiner le bien-fondé du système bancaire ouvert. Des initiatives du secteur privé impliquant des participants du secteur public ont également été de l'avant; pensons au travail du CCIAN sur le Cadre de confiance pancanadien, au lancement du groupe de travail canadien du Financial Data Exchange (FDX) et au travail du Conseil Stratégique des DPI sur les normes de système bancaire ouvert, en collaboration avec Open Banking Initiative Canada (OBIC) et FDX. Plus récemment, en février 2021, le Comité permanent des finances de la Chambre des communes publiait un rapport comportant des recommandations pertinentes, comme la recommandation 128, qui porte sur la mise en œuvre d'un système d'identité numérique qui donnerait à la population le pouvoir de garder la main haute sur les données qui la concernent détenues par le gouvernement fédéral, et la recommandation 129, qui préconise l'adoption d'une stratégie nationale de données[40].

Selon le CCIAN, les consommateurs, les entreprises et les entités gouvernementales doivent travailler ensemble à l'atteinte d'un objectif commun : la création d'un écosystème de l'identité numérique sûr, sécuritaire et fiable au Canada[41]. Il faut en faire une priorité absolue pour les décideurs, politiciens et chefs d'entreprise doivent prioriser l'identification numérique, afin que l'administration publique se donne une politique sur l'identification numérique au gouvernement, que le libellé de cette politique prévoie une identification numérique fiable et que les entreprises soient incitées à explorer des solutions numériques. Notons d'ailleurs que 83 % de la population fait confiance aux administrations publiques et 81 % aux institutions financières pour protéger ses données[42]. La collaboration entre secteurs public et privé dans ce dossier est essentielle; ainsi, 66 % de la population souhaite voir le gouvernement et les entreprises travailler ensemble à l'élaboration d'un cadre commun de l'identité

36 CCIAN. « L'impact économique de l'identité numérique au Canada ». https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.
37 Ministère des Finances du Canada. *Examen des mérites d'un système bancaire ouvert.* https://www.canada.ca/fr/ministere-finances/programmes/consultations/2019/systeme-bancaire-ouvert.html.
38 Susan Crutchlow, TransUnion. « Digital Identity – A Key Driver of Canada's Digital Economy ». https://www.transunion.ca/blog/digital-identity.
39 Sénat du Canada Rapport du Comité sénatorial permanent des banques et du commerce. *Un système bancaire ouvert, qu'est-ce que cela signifie?* https://www.sencanada.ca/fr/info-page/parl-42-1/banc-systeme-bancaire-ouvert/.
40 Chambre des communes. *Investir dans l'avenir : Priorités pour la croissance et la relance économiques*, rapport du Comité permanent des finances. https://www.noscommunes.ca/DocumentViewer/fr/43-2/FINA/rapport-1/page-21.
41 CCIAN. « L'impact économique de l'identité numérique au Canada ». https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.
42 CCIAN. *Les Canadiens sont prêts à adopter l'identité numérique*. https://diacc.ca/fr/2019/10/15/les-canadiens-sont-prets-a-adopter-lidentite-numerique/.

numérique[43]. Les retombées seraient considérables : les gouvernements fédéral, provinciaux et territoriaux pourraient créer ensemble les identifiants numériques, les entreprises joueraient un rôle actif dans leur élaboration et leur utilisation et il y aurait reconnaissance mutuelle et interopérabilité entre les participants du secteur public et ceux du secteur privé. L'application de normes aurait également pour effet de prévenir l'utilisation frauduleuse de renseignements personnels des clients et de fixer des règles strictes de confidentialité et de sécurité balisant les renseignements et les données personnelles des clients.

La population réclame un meilleur contrôle de ses données et un accès plus facile; au Canada, 9 personnes sur 10 sont en faveur de l'identification numérique et la grande majorité croit qu'elle est importante pour l'économie numérique[44]. Au pays, des millions de personnes partagent déjà des renseignements bancaires avec des fournisseurs tiers; or en l'absence d'un régime officiel de système bancaire ouvert, elles sont contraintes de recourir à des méthodes moins sécuritaires (partage de mot de passe bancaire en ligne avec d'autres fournisseurs de services financiers), au risque de compromettre leur identité personnelle et la confidentialité de leurs renseignements financiers. Un système officiel d'identité numérique qui irait de pair avec le régime de système bancaire ouvert faciliterait grandement l'authentification, à la fois pour les consommateurs et les fournisseurs de services : les premiers seraient en mesure de ne partager que les renseignements requis pour les authentifier sans avoir à utiliser des mots de passe susceptibles d'être volés, tandis que les seconds seraient sûrs de la validité de l'identifiant utilisé pour accéder aux renseignements de leur client et n'auraient plus à se soucier des vols de mot de passe. Les solutions de rechange, de même que l'utilisation de mots de passe et de questions de sécurité volables, posent un important risque pour la sécurité. L'absence d'identité numérique et de système bancaire ouvert compromet la sécurité de la population et de ses données. Un cadre d'identité numérique canadien présente un **potentiel d'économies nettes par établissement d'au moins 100 millions de dollars canadiens par année, grâce à l'efficacité opérationnelle… et à la réduction de la fraude**[45]. Compte tenu de ces défis, la normalisation est une solution possible pour la mise en œuvre d'un cadre d'identité numérique au Canada à l'image des valeurs de la population (inclusion, transparence et confiance).

De nos jours, les grandes entreprises de technologies cernent précisément les goûts et centres d'intérêt des gens[46]; les institutions financières connaissent leurs centres d'intérêt et habitudes de consommation; et les ministères et organismes gouvernementaux connaissent leurs renseignements biographiques. Les seuls à ne pas pouvoir les consulter sont les personnes et entreprises que ces données concernent.

Au Canada, des services d'authentification numérique sont déjà utilisés; pensons notamment à Vérifiez.Moi par SecureKey, utilisé par des ministères, des fournisseurs de soins de santé, des institutions financières et des entreprises de technologie financière (p. ex. accès à Service Canada ou à l'ARC, production de déclarations de revenus en ligne ou services bancaires en ligne). Des provinces comme l'Alberta et la Colombie-Britannique ont déjà leur propre système d'identification numérique, et l'Ontario et le Québec ont commencé à aller de l'avant avec les leurs. Toutefois, en l'absence d'un cadre national de gestion de l'identité appuyé par une normalisation et une réglementation robustes, le fonctionnement actuel de l'identification numérique au pays présente des défis. La fragmentation des identités en ligne entre de nombreuses entreprises et entités accroît le risque systémique de fraude par accumulation de données. Résultat : des atteintes à la sécurité des données qui minent la confiance des gens envers les organisations touchées et l'économie numérique[47]. Traditionnellement, l'identité se prouvait au moyen de documents physiques (passeports, cartes d'identité, etc.). Or ces documents peuvent être contrefaits ou modifiés, et la fraude entraîne des pertes financières importantes. De plus, bon nombre de personnes n'ont pas les moyens de prouver leur identité, ce qui les empêche d'accéder facilement à des services numériques, comme les soins de santé, les services gouvernementaux et les services bancaires, une situation mise en lumière par la pandémie. Selon un récent sondage du CCIAN, 75 % de la population serait d'avis que la COVID-19 a rendu l'identité numérique « bien plus importante » ou « un peu plus importante », tandis que seulement 2 % croit qu'elle est « bien moins importante »[48].

43 CCIAN. 2020. https://diacc.ca/fr/2021/02/16/la-covid-19-a-accelere-la-demande-des-canadiens-pour-une-identite-numerique/.
44 CCIAN. 2020.https://diacc.ca/fr/2021/02/16/la-covid-19-a-accelere-la-demande-des-canadiens-pour-une-identite-numerique/.
45 CCIAN. « Industry Insights: Digital ID in Financial Services ». https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.
46 Jathan Sadowski, *The Guardian*. « Companies are making money from our personal data – but at what cost? ». https://www.theguardian.com/technology/2016/aug/31/personal-data-corporate-use-google-amazon
47 CCIAN. « L'impact économique de l'identité numérique au Canada ». https://diacc.ca/news/the-economic-impact-of-digital-identity-in-canada/.
48 CCIAN. 2020. https://diacc.ca/fr/2021/02/16/la-covid-19-a-accelere-la-demande-des-canadiens-pour-une-identite-numerique/.

La pandémie a limité les interactions en personne, de sorte que les institutions et secteurs traditionnels ont dû réagir immédiatement pour se restructurer et s'adapter à la réalité de la concurrence numérique. Le gouvernement devrait pouvoir tirer profit de l'identité numérique et du système bancaire ouvert pour répondre à certaines priorités (PCU, ProGen RH et paie et modernisation du régime de pension, entre autres). Cependant, l'absence de réglementation et de normes encadrant des outils adaptés pour y parvenir, tels que l'identité numérique, porte préjudice à la population sur les plans économique et concurrentiel, et plus important encore, en matière de sécurité. Selon une étude de McKinsey, l'identification numérique complète pourrait libérer une valeur économique équivalant à 3 à 6 % du PIB en 2030 en moyenne[49], soit environ 48 à 97 milliards de dollars canadiens.

Plusieurs pays ont une bonne longueur d'avance sur le Canada. Pensons à l'Australie qui, dans le cadre d'un plan de relance économique postpandémie, a récemment annoncé un investissement de 256,6 millions de dollars australiens (environ 243 millions de dollars canadiens) destinés à un système d'identité numérique[50]. Parallèlement, l'Union européenne (UE) a adopté une réglementation sur l'identification électronique et les services de confiance (règlement eIDAS) qui permet une reconnaissance mutuelle des moyens d'identification numérique des organismes du secteur public des États membres de l'UE. Ce règlement, adopté aux Pays-Bas, autorise les citoyens et citoyennes à accéder à des services publics dans d'autres États membres de l'UE au moyen d'une clé de connexion nationale (comme DigiD)[51] », et ceux et celles d'autres pays de l'UE à utiliser leur propre système d'identité numérique nationale pour accéder aux services publics. Le règlement eIDAS prévoit déjà divers niveaux d'assurance pour l'identification, mais le gouvernement néerlandais a conçu un cadre d'identité numérique comportant un niveau encore plus élevé d'assurance[52]. Son cadre tient compte de 14 principes directeurs universels, dont le droit à l'identité numérique, la définition de l'utilisation par les personnes physiques et morales des secteurs public et privé, la protection de la vie privée, le respect des normes nationales et internationales, la flexibilité des infrastructures, la place de l'innovation et la garantie d'une surveillance indépendante. Le gouvernement néerlandais a également clarifié son rôle par rapport à l'infrastructure d'identification numérique : légiférer, élaborer des politiques, appliquer des pénalités, tenir les registres, fournir des services (gouvernementaux), soutenir la création d'outils d'identité numérique et financer l'infrastructure[53].

Citons également l'Estonie, généralement reconnue comme un modèle d'excellence en la matière, où citoyens et résidents peuvent obtenir et partager leurs données. Depuis plus de 15 ans, le gouvernement leur fournit une identification numérique leur donnant accès à divers services en ligne[54]. Cette identité électronique est assortie d'une carte physique. Utilisée pour l'identification électronique, la signature électronique et le transfert sécuritaire de données confidentielles, elle est aussi efficace que l'identification en personne. Les citoyens et les résidents permanents s'en servent pour accéder à l'ensemble des services numériques publics et de nombreux services privés – banques, télécommunications, sociétés énergétiques, et bien d'autres – de manière sécurisée. Les Estoniennes et les Estoniens y ont recours pour leurs déclarations d'impôts (une formalité qui prend généralement trois minutes), le vote, les soins de santé, les prescriptions, l'éducation, l'enregistrement de biens-fonds et l'enregistrement d'entreprises (en 15 minutes)[55]. Leur carte peut également être utilisée dans des épiceries, les librairies, les pharmacies, les bibliothèques, les cinémas… Il leur est possible de transférer des données confidentielles par courriel ou sur des plateformes de partage de fichiers en toute sécurité, sans risque de compromettre leur confidentialité et leur intégrité, le tout de manière efficace et peu coûteuse. L'identification électronique nationale est largement utilisée et acceptée par les secteurs public et privé, qui ont confiance en ce système où les services sécurisés électroniques font maintenant partie du quotidien, faisant gagner temps et argent aux citoyens, aux entreprises et au secteur public[56].

Il est à noter que ces pays diffèrent du Canada, et que leurs approches ne conviendraient pas nécessairement au contexte canadien. On peut toutefois en tirer d'importantes leçons à appliquer aux politiques nationales, comme l'intégration de l'identité numérique à la législation dans le but de favoriser son acceptation par les

49 McKinsey Global Institute. *Digital Identification: A key to inclusive growth*. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth.

50 Premier ministre de l'Australie. *Digital Business Plan to Drive Australia's Economic Recovery*. https://www.pm.gov.au/media/digital-business-plan-drive-australias-economic-recovery.

51 Gouvernement des Pays-Bas. « Everything you need to know about eIDAS ». https://www.government.nl/topics/online-access-to-public-services-in-the-european-union-eidas/everything-you-need-to-know-about-eidas.

52 Gouvernement des Pays-Bas, ministère des Affaires intérieures et des Relations au sein du Royaume. « Digital Identity Vision: Building Trust in the Digital World », présenté par Dick Dekkers (Digidentity) au CCIAN le 23 février 2020.

53 Gouvernement des Pays-Bas, ministère des Affaires intérieures et des Relations au sein du Royaume. « Digital Identity Vision: Building Trust in the Digital World », présenté par Dick Dekkers (Digidentity) au CCIAN le 23 février 2020.

54 e-Estonia. « Watch how the eID makes life easier in Estonia ». https://e-estonia.com/eid-in-estonia/.

55 Startup Estonia. « Why Estonia? ». https://startupestonia.ee/why-estonia.

56 e-Estonia. « Watch how the eID makes life easier in Estonia ». https://e-estonia.com/eid-in-estonia/.

entités publiques et privées de même que l'utilisation du système d'identité numérique et des infrastructures d'information numérique par les citoyens, les entreprises et les gouvernements. Ces exemples à l'international illustrent bien la situation d'autres pays et permettent de mesurer les risques que le Canada perde du terrain.

Bien que le ministère des Finances ait tenu en 2019 une consultation sur les « mérites d'un système bancaire ouvert », parallèlement au lancement de la Charte canadienne du numérique, le Canada accuse toujours du retard lorsqu'il s'agit de faire le lien entre les pièces d'identité délivrées par le gouvernement et les identifiants numériques, ce qui pourrait promouvoir une sécurité améliorée et une meilleure expérience client. Étant donné la nature des renseignements confidentiels susceptibles d'être échangés ou stockés, les questions de confidentialité et de cybersécurité devraient être au cœur des priorités du gouvernement, de l'industrie et des intervenants concernés.

Si le Canada n'a pas de structure officielle de système bancaire ouvert, il y existe cependant une structure informelle où les gens partagent de l'information avec des tiers sans y être autorisés, ce qui entraîne des risques importants pour la protection, la vie privée et la cybersécurité des consommateurs. À titre d'exemple, le ministère des Finances du Canada estime qu'actuellement, près de quatre millions de personnes accèdent à leurs données financières au moyen d'applications tierces comme les agrégateurs de données qui colligent de l'information pour produire un instantané de la situation financière d'un client[57]. Ce procédé implique que les clients transmettent leur identifiant bancaire en ligne à une application tierce, ce qui ne respecte pas les modalités énoncées par la plateforme bancaire en ligne en plus d'être moins sécuritaires. Bien que la législation sur la confidentialité s'applique à la collecte, à la conservation et à la gestion d'information effectuées par les établissements tiers, les consommateurs n'ont pas toujours de garantie quant au respect de ces exigences ou ne les comprennent pas toujours bien (même lorsque les tiers expliquent clairement comment la sécurité et la confidentialité des données sont préservées). Les clients ne savent parfois pas comment vérifier si les services externes conservent leurs données en sécurité et, advenant le cas d'une violation de données, ne disposent pas de mécanismes pratiques pour déposer une plainte ou obtenir une compensation. Malgré cet état de fait, près de 50 % de la population se dit prête à transmettre des renseignements personnels à une institution financière en échange de meilleurs produits et services[58].

Les acteurs des secteurs public et privé reconnaissent que les Canadiens et Canadiennes se transmettent déjà des données, et que souvent, cette transmission n'est pas aussi sécurisée que dans un vrai système bancaire ouvert. C'est pourquoi il est essentiel de protéger la confidentialité et la sécurité de la population par une structure de partage de données sécuritaire. La mise en place d'un tel cadre de partage de données et de système bancaire ouvert portera ses fruits. Nombreux sont ceux qui recherchent déjà des services pour mieux comprendre et gérer leurs finances, notamment par une comparaison des produits financiers facilitée, des offres de produits financiers personnalisés, et l'agrégation des paies et de la comptabilité[59]. Un système bancaire ouvert stimulera la concurrence dans le secteur, ce qui se traduira par de meilleurs produits et des services plus efficaces, le tout dans une structure fiable digne de confiance où les droits sur les données, le consentement et la protection du consommateur seront respectés, et où la surveillance réglementaire sera adéquate. Les utilisateurs du système pourront partager des données financières avec les institutions qui satisfont aux critères pour en faire partie, ce qui leur permettra de faire confiance à ces institutions et leur donnera la possibilité de porter plainte et d'obtenir une compensation en cas de problème. Beaucoup arrêteront de se rendre en succursale pour n'utiliser que les services financiers en ligne, mais d'autres continueront d'utiliser des services bancaires téléphoniques ou en personne. L'expérience de tous sera bonifiée par la possibilité d'accéder à des services bancaires de la manière qui leur convient.

Le rapport du Sénat du Canada sur les services bancaires ouverts fait état des avantages économiques d'un tel système, qui « favoriser[a] la croissance et l'innovation dans le secteur de la technologie financière. [...] S'il ne saisit pas maintenant l'occasion de créer un environnement réglementaire propice à un système bancaire ouvert, le Canada risque de prendre du retard par rapport à d'autres pays[60] ». Les institutions financières du pays (banques, technologie financière, etc.) courent le risque de ne pas pouvoir se mesurer à celles de pays qui ont un système bancaire ouvert. Si le Canada va de l'avant avec un tel système, nos entreprises pourront non seulement concurrencer leurs rivales internationales, mais également s'ériger en chefs de file des services financiers[61].

57 Rapport du Comité sénatorial permanent des banques et du commerce. Un système bancaire ouvert, qu'est-ce que cela signifie? https://www.sencanada.ca/fr/info-page/parl-42-1/banc-systeme-bancaire-ouvert/.

58 Robert Vokes et Andrew McFarlane, The Globe and Mail. « Canadian banks need to prepare for open banking now or risk being left behind ». https://www.theglobeandmail.com/business/commentary/article-canadian-banks-need-to-prepare-for-open-banking-now-or-risk-being-left/.

59 Ministère des Finances du Canada. *Examen des mérites d'un système bancaire ouvert.* https://www.canada.ca/fr/ministere-finances/programmes/consultations/2019/systeme-bancaire-ouvert.html.

60 Sénat du Canada. Rapport du Comité sénatorial permanent des banques et du commerce. *Un système bancaire ouvert, qu'est-ce que cela signifie?* https://www.sencanada.ca/fr/info-page/parl-42-1/banc-systeme-bancaire-ouvert/.

61 Ministère des Finances du Canada. *Examen des mérites d'un système bancaire ouvert.* https://www.canada.ca/fr/ministere-finances/programmes/consultations/2019/systeme-bancaire-ouvert.html.

En ce qui concerne le système de normalisation en tant que tel, aucun des grands organismes de normes internationales n'a publié de normes propres au système bancaire ouvert. Des organismes d'élaboration de normes (OEN) du Canada, comme le Conseil Stratégique des DPI, ont commencé l'élaboration d'une série de normes en la matière (CAN/CIOSC 110-x). De plus, FDX, une association d'entreprises américaines présente au Canada, a publié une norme sur les API[62] qui encadre l'accès aux données financières de plus de 12 millions de consommateurs[63]. Sans cadre formel de système bancaire ouvert, le Canada devra chercher des exemples à l'international des travaux et des approches des pays qui ont mis en œuvre leur propre système bancaire ouvert. Il gagnerait à s'inspirer de l'initiative de système bancaire ouvert du Royaume-Uni (OBIE), de la Directive sur les services de paiement 2 (DPS 2), de la Singapore Financial Data Exchange (SGFinDex) et de la loi australienne sur les droits des consommateurs par rapport à leurs données dans le but d'analyser les approches adoptées ailleurs et d'en tirer des pratiques exemplaires applicables au Canada. À l'instar de certains de ses homologues, il pourrait adopter la méthode du bac à sable. C'est ce qu'a fait l'OBIE pour que ses développeurs connectent leurs applications aux API afin de les tester et de mieux comprendre les outils, les normes et les exigences de sécurité qui s'appliquent au système bancaire ouvert[64].

Il faut noter l'important travail de normalisation accompli en ce qui a trait à l'identité, aux identifiants et à la fiabilité numériques par des OEN canadiens et des OEN internationaux, et notamment les publications et directives rédigées par des consortiums et des associations industrielles. Au Canada, le Groupe CSA et le Conseil Stratégique des DPI ont tous deux travaillé sur des normes liées à la fiabilité et à l'identité numériques, tandis qu'à l'international, l'ISO, l'IEC, l'UIT-T, l'IEEE, l'ETSI, le NIST et le W3C ont publié de nombreuses normes sur le sujet et sur des technologies liées aux identifiants, mais aucune ne porte spécifiquement sur l'identité numérique ou le secteur bancaire ouvert (on trouvera un survol des normes et organisations pertinentes à la fin du présent rapport, ainsi qu'une liste des acronymes et une description des organisations à l'annexe F de la feuille de route).

Nous devons ajouter nos voix au travail de normalisation en cours à l'international dans ces divers organismes de normalisation afin de faire la promotion de l'innovation et de la propriété intellectuelle de notre pays. C'est avec la participation des secteurs public et privé à l'élaboration de normes que les entreprises canadiennes pourront ouvrir des débouchés et générer des revenus à l'échelle nationale et internationale.

Malheureusement, malgré les progrès dans l'utilisation de technologies novatrices (chaînes de blocs, IA) la population doit encore se fier, pour certains services, à des systèmes analogiques ou manuels, dont l'utilisation s'avère chronophage et frustrante, ou à des services numériques qui privilégient la praticité au détriment de la sécurité, comme certains systèmes de vérification d'identité et de comptes. La COVID-19 a mis encore davantage en lumière l'importance de disposer de solutions entièrement numériques et à distance. Par exemple, avant les changements récents apportés par le Centre d'analyse des opérations et déclarations financières du Canada visant à permettre l'ouverture de comptes entièrement à distance, certaines institutions permettaient à leurs clients de commencer l'ouverture de comptes en ligne, mais leur demandaient ensuite de prendre rendez-vous avec un représentant pour vérifier leur identité en personne avant l'activation. Bien que la transition vers une expérience entièrement en ligne soit amorcée, certains services nécessitent encore que les clients fournissent des photos ou des pièces d'identité physiques à l'ouverture à distance d'un compte en ligne, malgré les risques de contrefaçon. De plus, les clients qui souhaitent transférer leurs comptes de placement d'une institution financière à l'autre dépendent d'institutions aux processus manuels et aux outils désuets (poste et télécopieur). Si l'envoi postal est égaré ou les résultats envoyés au mauvais numéro, les renseignements financiers confidentiels du client risquent de tomber en de mauvaises mains.

En ce qui a trait aux droits et au contrôle des consommateurs sur leurs données, et aux progrès technologiques qui s'y rattachent, des pays comme l'Estonie, les Pays-Bas et Singapour ont conçu l'équivalent d'un train à grande vitesse alors que le Canada peine à les suivre à bicyclette. Avec le temps, l'écart entre le train et le vélo s'accentue; pour rattraper son retard, le pays doit absolument monter à son tour dans un train à grande vitesse.

62 Financial Data Exchange. « Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5 ». https://www.newswire.ca/fr/news-releases/financial-data-exchange-adds-39-new-members-with-expanding-international-footprint-838469346.html.

63 Newswire. « Financial Data Exchange Adds 39 New Members with Expanding International Footprint ». https://www.newswire.ca/news-releases/financial-data-exchange-adds-39-new-members-with-expanding-international-footprint-838469346.html.

64 Initiative *Open Banking* du Royaume-Uni. « Developer Zone: Do you have test environments for PTP including a sandbox? ». https://openbanking.atlassian.net/wiki/spaces/DZ/pages/22872552/Do+you+have+test+environments+for+TPPs+including+a+sandbox.

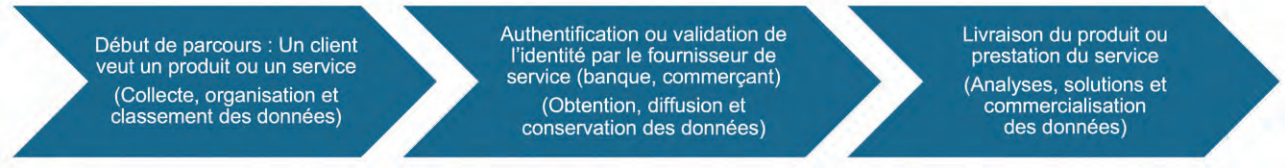
TÉMOIGNAGES D'UTILISATEURS

Pour tirer profit de la vaste expérience des membres du groupe de travail, on les a sondés afin de recueillir leurs commentaires sur le cycle de vie de l'identité numérique ou du système bancaire ouvert, d'un point de vue personnel ou organisationnel. En plus de répondre au sondage, les membres se sont prononcés sur les questions suivantes :

- Quels sont les ***risques de l'inaction*** du Canada s'il ne se dote PAS d'un cadre d'identité numérique ou d'un cadre de système bancaire ouvert?
- Dans un monde idéal, ***quelles microactions sont nécessaires pour aller de l'avant?***

Les membres devaient répondre en se basant sur le diagramme d'analyse du cycle de vie ci-dessous – l'expérience d'un utilisateur – et dire quel était l'avenir idéal qui créerait de la valeur pour la population.

Analyse du cycle de vie – cas d'usage de l'identité numérique et du système bancaire ouvert



Les membres qui ont étudié le cas d'usage sur l'identité numérique et le système bancaire ouvert ont échangé sur leur expérience personnelle ou organisationnelle du parcours des données : identité numérique, système bancaire ouvert, normalisation et intégration de valeurs chères aux Canadiens comme l'inclusion, la transparence et la confiance. Le groupe a notamment soulevé un défi de taille : la piètre compréhension des effets de l'identité numérique et du système bancaire ouvert dans la vie de tous les jours. Voici quelques témoignages représentatifs des concepts et des récits exposés par les experts du groupe de travail.

LE DEUIL D'UN ÊTRE CHER ET SES CONSÉQUENCES

Une veuve doit composer avec le processus complexe et la montagne de tâches qui accompagnent le règlement de succession de son mari décédé. Elle doit être désignée légalement comme liquidatrice, un processus à refaire pour chaque institution (gouvernementale, bancaire, etc.). Aujourd'hui, la succession est un processus difficile, complexe et épuisant sur le plan émotionnel, et l'est d'autant plus lorsqu'une personne vit un deuil difficile.

Le processus serait grandement facilité par une vérification en ligne fiable (plutôt qu'en personne, par la poste ou au téléphone) et la possibilité de partager des données entre des institutions de confiance. Ainsi, la personne qui souhaite être désignée comme liquidatrice n'aurait qu'à montrer une pièce d'identité une fois aux fins de vérification, puis pourrait ensuite se charger de la succession auprès de toutes les institutions financières et tous les ordres de gouvernement. Les tâches de liquidateur ou de procuration et la charge physique et émotionnelle du processus actuel en seraient grandement allégées.

LE PAIEMENT DU LOYER

Un propriétaire perçoit les loyers d'un locataire. Le processus est simple pour les deux personnes concernées : habituellement, le locataire donne un chèque annulé au propriétaire, qui le transmet à la banque. L'enjeu ici réside dans la quantité de renseignements personnels que le locataire doit transmettre, soit son numéro de compte bancaire. Le locataire n'a pas de contrôle sur l'utilisation ou la conservation de ces données lorsque le chèque annulé se retrouve entre les mains du propriétaire.

Les locataires auraient plus de pouvoir sur la nature des données transmises et stockées et les modalités, et les paiements préautorisés pourraient être effectués sans que soit transmise plus d'information que nécessaire.

ACCÈS AUX DONNÉES FINANCIÈRES PERSONNELLES POUR UTILISATIONS SECONDAIRES

Les consommateurs doivent avoir accès à leurs données financières personnelles et transactionnelles à plusieurs fins. Cet accès pose toutefois des risques pour la sécurité, comme l'utilisation frauduleuse d'appareils, l'hameçonnage et le vol d'identité.

Le pouvoir des consommateurs sur leurs propres données leur permettrait d'accéder à divers services visant à les aider à prendre de meilleures décisions tout en améliorant la sécurité des données et la concurrence sur le marché. Des connexions à l'identité numérique pourraient également pallier les risques actuels pour la sécurité.

UNE GESTION PLUS EFFICACE DES FINANCES PERSONNELLES ET DES FINANCES D'ENTREPRISES

Une personne pourrait vouloir gérer ses finances personnelles plus facilement en rassemblant l'ensemble de ses comptes et de ses actifs sur une plateforme conviviale.

Une entreprise comme une coopérative de fabricants pourrait gérer son travail administratif et ses finances de manière encore plus sécuritaire grâce à l'identité numérique et au système bancaire ouvert.

Grâce à l'identité numérique, les institutions auraient l'assurance que seules les personnes autorisées prennent des décisions, et grâce au système bancaire ouvert, les utilisateurs, les entreprises et les gouvernements pourraient partager des données comme bon leur semble, de façon plus sécuritaire et efficace qu'avec les méthodes actuelles.

Un thème revient d'un témoignage à l'autre : les difficultés actuelles liées au partage et à l'obtention des données, et à leur conservation à un emplacement unique. Dans le cas du propriétaire et du locataire, c'est l'inverse : le locataire partage trop de données et ne sait pas comment le propriétaire les conservera.

En l'absence de cadres d'identification numérique et de service bancaire ouvert, la population a le choix : se reposer sur des technologies analogiques désuètes ou, par volonté d'efficacité, compromettre sa sécurité en transmettant des mots de passe en ligne ou en envoyant des images de ses renseignements personnels par des méthodes peu sécurisées. Au fardeau économique s'ajoute un lourd fardeau émotionnel. Lorsqu'ils doivent entreprendre des processus administratifs inefficaces et fastidieux, la frustration monte chez les utilisateurs habitués à faire des choses en ligne rapidement.

L'identité numérique inspirerait confiance dans l'authentification d'une personne ou de plusieurs personnes d'une organisation et la mise en place d'un partage de données plus rapide, sécuritaire et efficace. Quant au service bancaire ouvert, il donnerait aux consommateurs un meilleur contrôle de leurs données et leur permettrait d'utiliser et de partager leurs données financières plus efficacement, améliorerait la prise de décisions et la sécurité, et favoriserait la concurrence. Tous deux concourraient au remplacement de l'ancienne infrastructure, peu conviviale, par de nouvelles avancées technologiques.

RÉSULTATS DU SONDAGE

Les répondants ont lu chacun des témoignages et les ont classés selon quatre grands thèmes.

1. Fondements de la gouvernance des données en matière d'identité numérique et de système bancaire ouvert

On a demandé aux répondants d'étudier les pratiques actuelles lorsqu'une personne commence à utiliser un produit ou un service, comme à l'ouverture d'un compte ou au début d'une transaction. Par exemple, comment une organisation peut-elle établir hors de tout doute l'identité d'un client, et comment un client peut-il confirmer l'identité d'un fournisseur de service? La réglementation actuelle permet-elle l'utilisation de l'identité numérique pour une transaction? En tant que consommateur, à quel point peut-on faire confiance à l'organisation à qui les données sont transmises, et sur quelle base? Comment savoir si ces données sont utilisées à d'autres fins? Les fournisseurs de service réutilisent-ils les données, et si oui, à quelles fins? Les clients sont-ils au courant?

Les répondants se sont également prononcés sur l'avenir souhaité. Par exemple, quelles macroactions faut-il entreprendre pour tirer profit de l'identité numérique et du service bancaire ouvert? Quel est le rôle de la normalisation et de la réglementation? Que faut-il faire pour que l'interopérabilité soit fondamentale?

Concernant les fondements de la gouvernance des données et la situation actuelle, les participants ont mentionné qu'il est difficile d'obtenir ou de partager les données nécessaires et que la plupart du temps, l'identité numérique n'est pas une option. Les pièces d'identité physiques demeurent la méthode d'identification la plus courante, non sans risques de contrefaçon. En l'absence d'un système d'identité numérique, il est impossible d'effectuer certaines tâches en ligne, tandis que d'autres accordent une importance et une confiance démesurées aux mots de passe. Des processus administratifs qui pourraient être effectués beaucoup plus simplement en ligne s'avèrent d'une lourdeur et d'une difficulté exagérées.

Des experts ont également ciblé les principaux problèmes de sécurité des données. La réputation de certaines institutions (gouvernements, institutions financières et fournisseurs de soins de santé) inspire confiance au public. Des règlements sur la protection des données empêchent leur transmission à des tiers, mais malheureusement, il y a de nombreuses autres situations où les organisations n'ont pas mis en place de dispositifs de confidentialité ou de protection des données, et où des atteintes ont été constatées. Par ailleurs, certaines organisations font l'objet d'une certaine méfiance, attribuable notamment à la complexité délibérée des contrats d'utilisation, et à des histoires de fraude et d'utilisation malveillante de données dans les manchettes.

Un autre problème majeur découle du manque de contrôle des utilisateurs sur leurs données. Nombre de fournisseurs de service utilisent et analysent les données du consommateur pour créer de la valeur à la fois pour eux-mêmes et pour celui-ci. Le consommateur le sait (à condition de lire les modalités de service), mais n'a pas la possibilité de demander l'anonymat, de bloquer les publicités liées à ses données ou de partager ces données.

Les participants sont en faveur de l'adoption de l'identité numérique et du système bancaire ouvert, qui créerait des méthodes d'accès et de gestion des données en ligne. Tous deux généreraient beaucoup de valeur pour le public, par la simplification des processus, un gain de temps et une réduction des coûts, entre autres. Le soutien et la mise en œuvre par tous les ordres de gouvernement et grandes institutions du secteur privé favoriseraient une adoption à grande échelle et l'abandon de processus archaïques (télécopieurs et documents papier).
Les normes favoriseraient la confidentialité, la sécurité et l'interopérabilité entre les nouveaux et les anciens systèmes, et créeraient un environnement propice aux innovations. Les normes sur la classification, le partage, le traitement et la conservation des données contribueraient à la cohérence de la mise en œuvre et à l'inclusion des fournisseurs de service, sans dépendre d'une technologie en particulier.

2. Entreprendre une activité en ligne (collecte, organisation et classement de données)

Les répondants ont dû décrire, selon leur point de vue et leur expérience, le type de renseignements requis pour établir l'identité. Les questions portaient notamment sur les méthodes de collecte et le lieu de conservation des données, ainsi que sur les préoccupations concernant la qualité des données recueillies et le statut du cadre de documentation (normes, pratiques exemplaires et certifications).

Les questions sur l'avenir souhaité portaient sur le type de renseignements, selon le point de vue et l'expérience des répondants, qui devraient être demandés pour vérifier l'identité et la façon dont l'identité numérique permettrait d'y arriver.

Actuellement, la vérification de l'identité se fait généralement au moyen de document physique et implique souvent des interactions en personne. D'ordinaire, plusieurs pièces d'identité sont requises et la plupart de ces processus sont inefficaces. Des copies électroniques de documents physiques sont parfois utilisées, mais ne sont pas toujours envoyées de manière sécuritaire. Certains clients envoient des documents par courriel, un processus sécuritaire à condition que le courriel soit chiffré (la plupart des gens ignorent comment le faire). Il y a eu des progrès dans les technologies d'authentification (NIP, authentification à deux facteurs, authentification biométrique, etc.).

Dans l'avenir souhaité, l'identité numérique et le système bancaire ouvert permettraient une diffusion simple et sécuritaire des données à diverses fins et donneraient aux consommateurs le plein contrôle de leurs données afin de gérer les diverses situations de la vie, leurs finances, etc. Les renseignements nécessaires seraient transmis, sans plus. Les secteurs public et privé participeraient à ce système, soumis à une surveillance appropriée. Il faudrait une grande campagne de sensibilisation sur les droits de la population et l'utilisation de l'identité numérique et du système bancaire ouvert, car seulement près de la moitié des Canadiens et des Canadiennes se disent assez au courant du principe de l'identité numérique[65]. Les citoyens pourraient agréger plus facilement leurs données et prendre de meilleures décisions financières, tandis que les entreprises tireraient profit de la réduction de leurs besoins en ressources, de la simplification de la vérification des fournisseurs et d'une diminution de la fraude.

3. API publique, données bancaires, applications bancaires : où s'en vont les données? (accès, diffusion et conservation des données)

On a posé aux répondants des questions sur les pratiques actuelles : qui a accès aux données des clients (à l'interne et à l'externe)? Ces données sont-elles partagées avec des tiers? Quelles normes ou pratiques de certification balisent le tout? De quoi l'avenir souhaité est-il fait?

Plusieurs institutions ont des règles strictes encadrant le traitement des données des clients, qui visent à ce que seul le personnel autorisé y ait accès. Les institutions financières ne transmettent pas de renseignements personnels identifiables à des tiers; toute donnée ainsi transmise pour une valeur ajoutée est masquée ou anonymisée en raison des exigences strictes des lois sur la confidentialité comme la *Loi sur la protection des renseignements personnels et les documents électroniques* (les organisations d'autres secteurs y sont également soumises).

S'ajoute à ces lois ISO 20022, une norme commune régissant l'échange de données et de messages de paiement entre les institutions financières, qui n'intègre toutefois aucune exigence de sécurité. En revanche, dans d'autres secteurs, le traitement des données n'est pas balisé par les mêmes règles, surtout lorsqu'il est question de processus manuels.

65 CCIAN. 2020. https://diacc.ca/fr/2021/02/16/la-covid-19-a-accelere-la-demande-des-canadiens-pour-une-identite-numerique/.

Plus des trois quarts des consommateurs se disent à l'aise avec le fait qu'on partage leurs données avec un tiers s'ils peuvent en retirer des avantages (bas prix, meilleur service)[66]. Ils ont toutefois des attentes élevées : contrôle complet de leurs données, possibilité de se retirer et transparence parfaite en ce qui concerne les entités qui accèdent à leurs données, les raisons de le faire et les mesures de sécurité visant à éviter qu'elles soient conservées ou exposées. Certains ont témoigné du soutien offert aux consommateurs, qui ont eu la possibilité de surveiller qui avait accès à leurs données et de comparer les services et les mesures de sécurité des fournisseurs, ce que permettraient les normes. Certains répondants se disent également en faveur de normes minimales encadrant la participation des institutions au système et l'établissement d'un programme d'évaluation de la conformité reconnu.

4. Produits et services (analyses, solutions et commercialisation de données)

Les dernières questions portaient sur ce que les fournisseurs tiers pouvaient faire avec les données auxquelles ils avaient accès (types d'analyse, destinataires autorisés de ces analyses, etc.). Que souhaitent les participants pour l'avenir? Par exemple, quels règlements ou normes pourraient stimuler la croissance des entreprises? Qu'est-ce qui freinerait les entreprises ou leur capacité de fournir un produit ou un service? Quels avantages pourraient en tirer les consommateurs et les fournisseurs de services canadiens?

Consommateurs et fournisseurs de services ont de multiples utilités et bienfaits à retirer de l'analyse de données : élimination de frictions dans divers processus, meilleure prise de décisions… L'identité numérique peut simplifier le processus de gestion du consentement, par exemple. Dans un système bancaire ouvert, les règlements fixeront la portée des données, les améliorations possibles et les modalités de partage.

Dans un avenir idéal, les services seraient plus rapides, simplifiés, moins chers, plus efficaces et transparents – que l'on pense à des paiements ou à une liquidation de succession, entre autres. Mieux éduqués, les consommateurs, qui auraient un meilleur contrôle de leurs données, seraient plus conscients de la valeur de ces dernières et s'impliqueraient davantage. Ils connaîtraient mieux les modèles de revenus des services qu'ils utilisent. Pour les parents, les tuteurs légaux et les proches aidants, l'identité numérique est un important outil qui les aiderait à gérer les soins de leurs enfants ou de leurs parents vieillissants, à faire le suivi des dossiers médicaux et des carnets de vaccination, à signer des formulaires de consentement, à s'inscrire à des programmes gouvernementaux ou à en remplir les formalités, à représenter quelqu'un légalement ou à agir par procuration[67].

Idéalement, l'adoption de l'identité numérique entraînerait des bienfaits importants pour la société, notamment en facilitant le fonctionnement du cadre de système bancaire ouvert par la réduction des risques et des inefficacités des systèmes et processus actuels. Les normes ont une grande importance pour l'atteinte de ces objectifs; elles peuvent notamment prévenir l'adoption de règlements trop prescriptifs qui freineraient l'innovation.

RÉSULTATS DES CONSULTATIONS PUBLIQUES

En décembre 2020, CCN et le Collectif ont consulté la population sur les thèmes de l'identité numérique et du système bancaire ouvert en organisant des séances de discussion – deux en anglais et une en français. Ces séances ont attiré plus de 100 participants de partout au pays, dont des représentants d'institutions financières et de fournisseurs de services tiers. Toutes ont commencé par un bref exposé des représentants du CCN sur le rôle du Collectif et l'importance des normes, suivi d'un état des lieux de l'identité numérique et du système bancaire ouvert au Canada. Les participants ont ensuite été invités à s'exprimer sur les deux grands thèmes suivants :

- l'état actuel de l'identité numérique et du système bancaire ouvert au Canada, notamment les possibilités et les défis actuels ainsi que les règles et les normes existantes;
- l'avenir idéal dans ces deux domaines : avantages souhaités pour les consommateurs, lois et règlements nécessaires à une structuration efficace de l'identité numérique et du système bancaire ouvert.

66 CCIAN. 2020. https://diacc.ca/fr/2021/02/16/la-covid-19-a-accelere-la-demande-des-canadiens-pour-une-identite-numerique/.
67 CCIAN. 2020. https://diacc.ca/fr/2021/02/16/la-covid-19-a-accelere-la-demande-des-canadiens-pour-une-identite-numerique/.

ÉTAT DES LIEUX ET DÉFIS ACTUELS

Pour lancer la discussion, une activité a été organisée autour d'un tableau blanc interactif pour amener les participants à exposer leurs points de vue sur les défis rencontrés au Canada dans les domaines de l'identité numérique et du système bancaire ouvert. Quatre grands thèmes récurrents sont finalement ressortis :

1. la confiance, plus précisément la nécessité de gagner et de conserver la confiance des consommateurs;
2. la sécurité, ou la nécessité de gérer les risques, de préserver la confidentialité et de prévenir la fraude;
3. la fragmentation, et la nécessité d'optimiser la coopération, l'interopérabilité et l'efficience;
4. une gouvernance et une surveillance efficaces, soit la nécessité d'établir des règles, des règlements et des normes cohérentes et harmonisées d'une province et d'un territoire à l'autre.

Après l'activité, les participants ont échangé en petits groupes. En réfléchissant à la situation actuelle de l'identité numérique et du système bancaire ouvert au Canada, la plupart ont estimé que le pays est extrêmement bien placé pour devenir un chef de file dans ces deux domaines. Toutefois, ils ont également convenu que le Canada prend du retard sur d'autres pays en ce qui concerne l'élaboration des cadres juridiques et réglementaires requis. De nombreux participants ont fait remarquer qu'il fallait davantage de leadership et de soutien du gouvernement fédéral dans ces domaines, car il n'existe actuellement aucune loi permettant et encadrant le développement du système bancaire ouvert au Canada. Parmi les autres lacunes évoquées par les participants, figure la sensibilisation et l'éducation des consommateurs, qui n'auraient pas les connaissances nécessaires pour utiliser en toute confiance l'identité numérique et le système bancaire ouvert. Cependant, il a également été noté qu'il revient aux administrations publiques et aux acteurs du secteur de faire connaître le système bancaire ouvert et de gagner la confiance des utilisateurs.

AVENIR IDÉAL

Les participants se sont ensuite penchés sur l'avenir souhaité en matière d'identité numérique et de système bancaire ouvert et ont globalement convenu que le consommateur devrait jouir d'un contrôle et d'un pouvoir décisionnel accrus sur l'accès et l'utilisation de ses données personnelles. Selon eux, un tel résultat passe par un changement de paradigme fondamental : une transition du contrôle institutionnel des données à un modèle plus transparent et démocratique, axé sur le consommateur – pouvoir décisionnel, priorité au client, interopérabilité et adoption. Ils ont imaginé un système national d'identité numérique complet et fiable fonctionnant de manière transparente à l'échelle nationale et provinciale. Par ailleurs, ils ont souligné que le succès était conditionnel à une utilisation et à une interopérabilité étendues des systèmes ainsi qu'à la mise en place de solides mécanismes de protection de la confidentialité.

RECOMMANDATIONS

À l'appui des sept principales recommandations énoncées dans la synthèse, les participants des consultations et les experts du cas d'usage s'entendent pour dire que le Canada a l'étoffe d'un chef de file mondial de la nouvelle technologie liée à identité numérique et au système bancaire ouvert, mais que l'absence des cadres légaux et réglementaires requis le relègue en queue de peloton. Plutôt que de viser la perfection, il lui faut mettre les bouchées doubles et corriger les principaux problèmes et inefficacités.

Le principal problème réside dans l'approche sur la confidentialité adoptée actuellement dans les lois canadiennes, qui considèrent les données d'un point de vue trop étroit, par exemple en encadrant la protection et la confidentialité sans traiter de la transmission. Les règlements ne donnent pas assez d'importance au contrôle des données par le consommateur et à son pouvoir de choisir qui y a accès de manière transparente, en intégrant ce contrôle à la confidentialité et à la protection des données. L'idée n'est pas celle d'un jeu à somme nulle; protection et transmission des données vont de pair avec maîtrise de la confidentialité, selon les principes de protection de la vie privée dès la conception.

Le Canada doit changer de cap et donner à ses citoyens et citoyennes un meilleur contrôle de leurs données. Il faut donc leur en donner le pouvoir, notamment quant aux autorisations d'accès, sans nuire aux droits à la vie privée ou à la sécurité des données; il s'agit plutôt de renforcer ces éléments en permettant à la population de les utiliser à sa guise pour ce qui lui importe.

En ce qui concerne les prochaines étapes, il est crucial que le Canada se mette en action le plus rapidement possible, s'appuyant sur ce qui a été fait par le passé et en mobilisant un large éventail de citoyens et de citoyennes et d'entreprises. Plus le Canada tarde à adopter l'identité numérique et le système bancaire ouvert, plus son écart avec les autres pays se creuse et risque de devenir impossible à combler.

De nombreux participants s'inquiètent des risques de l'inaction. Le Canada doit adopter une approche proactive le plus rapidement possible afin d'en tirer des avantages économiques et sécuritaires, mais également d'éviter ou d'atténuer les risques de l'inaction (retard par rapport aux autres pays, vulnérabilité aux attaques).

Plusieurs participants ont fait valoir que les Canadiens et les Canadiennes évoluent déjà dans un environnement bancaire ouvert : les gens transmettent des renseignements personnels, comme des mots de passe bancaires en ligne, pour permettre à de nouveaux services d'accéder à leurs données. Toutefois, rien n'encadre la protection des consommateurs et des données ni l'interopérabilité.

Pendant ce temps, l'absence de système d'identité numérique empêche la population d'utiliser des services en ligne de manière sécuritaire et les oblige à dépendre d'un système d'authentification désuet (pièces d'identité physique, photos de pièces d'identité, mots de passe et questions de sécurité), chronophage et non convivial qui pose des risques de contrefaçon et de fraude.

Pour le Canada, les risques s'articulent autour de trois axes : l'impossibilité pour la population de bénéficier d'un système d'identification en ligne et de transmission des données plus sécuritaire; un progrès technologique débridé qui irait dans plusieurs directions et empêcherait l'interopérabilité du système; et un frein à la compétitivité des innovateurs canadiens qui cherchent à développer leurs idées à l'international. Par son inaction, le pays serait rapidement dépassé par les innovateurs et les fournisseurs de service étrangers.

De nombreux experts du cas d'usage jugent que la collaboration entre les secteurs public et privé est essentielle pour aller de l'avant. L'adoption officielle par la normalisation des cadres nécessaires à l'identité numérique et au système bancaire ouvert semble la voie la plus prometteuse pour faire progresser rapidement et efficacement le Canada – et garantir sa sécurité.

PRINCIPAUX TERMES

Voici une liste des principaux termes et de la nomenclature utilisés dans le cadre du présent document pour faciliter la compréhension des témoignages présentés.

Authentification
Procédure de vérification des faits ou de l'authenticité visant à confirmer l'identifiant ou l'identité[68].

Consentement
Permission, accordée par un utilisateur autorisé, « de partager des renseignements identitaires et/ou personnels sur un sujet selon les modalités définies dans un avis[69]. »

68 CCIAN. *Proof of Concept – Online Proof of Residency.* https://diacc.ca/wp-content/uploads/2016/06/Online-Proof-of-Residency-POC-FINAL.pdf.
69 CCIAN. *Glossaire du CCP.* https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.

Identité numérique
Si l'identité est un ensemble d'indicateurs (ou d'attributs) sur une personne (entité) qui la rendent unique, l'identité numérique est un ensemble d'attributs qui permettent d'associer une entité personnelle à ses interactions virtuelles en utilisant des sources fiables un peu comme une empreinte en ligne.

Elle correspond également à l'information utilisée par les systèmes informatiques pour reconnaître une personne ou une organisation externe et lui donner un accès sécuritaire et efficace à des services numériques.

Elle donne plus de contrôle aux consommateurs sur leurs données et leur identité en leur permettant de choisir l'information à transmettre en fonction des besoins. Elle peut être normalisée et utilisée entre les entités, et on peut y ajouter de l'information[70].

Entité
« Chose ayant sa propre existence indépendante, comme une personne, une organisation ou un appareil, qui peut être assujettie à des lois, politiques ou règlements dans certains contextes, et qui peut avoir certains droits, devoirs et obligations[71]. »

Identité
« Renseignements physiques ou numériques sur un sujet qui l'identifient d'une façon unique dans un contexte, et qui sont utilisés exclusivement par ce même sujet, ou par une personne agissant pour le compte d'une organisation, pour accéder à des services en ligne avec confiance et assurance[72] »

Système bancaire ouvert (finances axées sur les clients)
Cadre de règlements et de normes « où les consommateurs et les entreprises peuvent autoriser des tiers fournisseurs de services financiers à avoir accès à leurs données sur leurs opérations financières au moyen de canaux sécurisés en ligne[73]. »

Organisation
Entité juridique « qui consiste en une personne ou un ensemble organisé de personnes ayant une vocation particulière et dont l'existence est établie par un statut juridique[74]. »

Personne
« Entité qui est un être humain biologique, vivant ou décédé[75] », « y compris les mineurs ou autres qui pourraient ne pas être reconnus comme des personnes à part entière par la loi[76]. »

Renseignements personnels
Tout « renseignement factuel ou subjectif, consigné ou non, concernant une personne identifiable[77]. »

Service
« Intervention, acte notarié ou effort de valeur accompli pour satisfaire un besoin ou répondre à une demande[78]. »

Normalisation
Élaboration et application de normes qui établissent les pratiques, les exigences techniques et la terminologie reconnues pour des produits, des services et des systèmes.

Les normes contribuent à améliorer la qualité, l'innocuité et l'efficacité des méthodes et des produits, et font partie intégrante de la technologie, de l'innovation et du commerce.

70 CCIAN. « L'impact économique de l'identité numérique au Canada ». https://diacc.ca/2019/07/18/diacc-industry-insights-digital-id-in-financial-services/.
71 Conseil stratégique des DPI Confiance et identité numérique – Partie 1 : Notions fondamentales. https://ciostrategycouncil.com/normes-2/confiance-numerique-et-de-lidentite-partie-1/?lang=fr.
72 CCIAN. *Glossaire du CCP.* https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.
73 Ministère des finances du Canada. *Examen des mérites d'un système bancaire ouvert.* https://www.canada.ca/fr/ministere-finances/programmes/consultations/2019/systeme-bancaire-ouvert.html.
74 CCIAN. *Glossaire du CCP.* https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.
75 CCIAN. *Glossaire du CCP.* https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.
76 Conseil stratégique des DPI Confiance et identité numérique – Partie 1 : Notions fondamentales. https://ciostrategycouncil.com/normes-2/confiance-numerique-et-de-lidentite-partie-1/?lang=fr.
77 CCIAN. *Glossaire du CCP.* https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.
78 CCIAN. *Glossaire du CCP.* https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.

Validation
« Processus qui confirme l'exactitude des renseignements sur l'identité numérique à propos d'un sujet tels qu'établis par une partie qui fait autorité[79]. »

Vérification
« Processus qui confirme que les renseignements sur l'identité numérique présentés sont reliés au sujet qui les affirme[80]. »

INITIATIVES DE NORMALISATION EN COURS

En ce qui a trait aux initiatives de normalisation, un important travail sur l'identité, les identifiants et la confiance numériques a été entrepris par des OEN canadiens et internationaux ainsi que des associations et consortiums industriels. Veuillez noter que cette liste n'est pas exhaustive et vise simplement à donner une idée du travail accompli.

Parmi les éléments ayant retenu notre attention, notons les normes Verified Credentials Data Model et *Web Authentication: An API for accessing Public Key Credentials Level 1*, ainsi que deux normes en cours d'élaboration, soit Credential Management Level 1 et *Web Authentication: An API for accessing Public Key Credentials Level 2*, publiées par W3C. Certains groupes de travail de l'organisme se penchent spécifiquement sur des normes sur l'identité, les identifiants et l'authentification, bien que son catalogue de normes soit moins fourni que celui du NIST et de l'UIT-T. Le NIST a publié des lignes directrices sur l'identité numérique :

- *Digital Identity Guidelines* (NIST SP 800-63-3);
- *Digital Identity Guidelines: Enrollment and Identity Proofing* (NIST SP 800-63A);
- *Digital Identity Guidelines: Authentication and Lifecycle Management* (NIST SP 800-63B);
- *Digital Identity Guidelines: Federation and Assertions* (NIST SP 800-63C).

L'UIT-T a lui aussi publié des cadres qui définissent les principes entourant l'identité numérique :

- *Cadre politique intégrant des principes applicables à l'infrastructure d'identité numérique* (UIT-T D.1140);
- *Cadre régissant le contrôle par l'utilisateur des identités numériques* (UIT-T X.1251);
- *Universal Authentication Framework* (UIT-T X.1277).

De nombreux organismes de normalisation s'impliquent de près ou de loin dans l'univers des TI et de la gestion de l'information : l'IEC, l'ISO, l'UIT-T, l'IEEE, le CEN et le CENELEC, l'ETSI, NIST, l'IETF et le W3C ont publié de multiples normes à ce sujet. L'ISO en a publié de nombreuses sur les TI, la sécurité, les chaînes de bloc, le management de la sécurité de l'information, et l'authentification; toutefois, aucune ne s'applique spécifiquement aux identifiants ou à l'identité numériques. L'IEEE a publié des normes sur la cryptographie, le chiffrage et les chaînes de bloc et de nombreuses autres normes sur le sujet sont en cours d'élaboration et portent sur les services numériques adaptés à l'âge, la gestion des données et les données ouvertes – notamment le *Standard for Blockchain-based Digital Identity System Framework*. En Europe, le CEN a publié des normes sur les systèmes de cartes d'identité, tandis que l'ETSI a des normes sur les signatures électroniques, les cartes intelligentes, la cryptographie, la gestion de l'identité et la gestion de l'accès. Des consortiums ont publié des protocoles et des normes complémentaires, comme les normes sur les protocoles Internet OAuth, JSON et SAML.

Au sein de ces entités, une multitude de comités techniques élaborent ces normes. À l'ISO, à l'UIT-T et à l'ETSI, par exemple, des comités techniques travaillent sur des sujets liés aux identifiants numériques, mais aucun ne se consacre précisément aux identifiants ou à l'identité. Étant donné sa portée technologique et ses orientations stratégiques, le comité technique du CEN sur l'identification des personnes et dispositifs à caractère personnel associés (CEN/TC 224) est l'un des plus importants à surveiller.

79 CCIAN. *Glossaire du CCP*. https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.
80 CCIAN. *Glossaire du CCP*. https://diacc.ca/wp-content/uploads/2020/09/Glossaire-du-CCP-Recommendation-Finale_V1.0.pdf.

Sur la scène nationale, le CCN accrédite 12 OEN soumis à un processus d'élaboration de normes strict qui requiert la participation d'un groupe diversifié d'intervenants (entreprises, milieu de la recherche, gouvernement et groupes de consommateurs), et travaille sur l'élaboration de normes par consensus. Deux des 12 OEN – l'Association canadienne de normalisation (Groupe CSA) et le Conseil Stratégique des DPI – ont publié des normes pertinentes à ce sujet, mais aucune ne porte encore précisément sur les identifiants numériques (bien que leur élaboration soit en cours, comme nous le décrivons ci-dessous). Le Groupe CSA a adopté un grand nombre de normes ISO sur les TI, la sécurité des TI et la cybersécurité, qu'il a publiées à l'intention du marché canadien. Il est également à noter que le travail accompli par le Groupe CSA est cité dans la *Loi sur la protection des renseignements personnels et les documents électroniques* et pourrait être cité dans de prochaines versions de la loi sur la confidentialité qui la remplacera. Bien qu'aucune de ces normes ne porte précisément sur les identifiants numériques, elles touchent tout de même à des sujets comme les cartes d'identité, l'authentification d'entités, la cryptographie et la protection des renseignements. En voici des exemples notables :

- *Techniques de sécurité IT – Authentification d'entité – Partie 3 : Mécanismes utilisant des techniques de signature numériques* (ISO/IEC 9798-3);
- *Technologies de l'information – Techniques de sécurité – Signatures numériques avec appendice – Partie 2 : Mécanismes basés sur une factorisation entière* (ISO/IEC 14888-2);
- *Technologies de l'information – Techniques de sécurité – Algorithmes de chiffrement – Partie 5 : Chiffrements identitaires* (ISO/IEC 18033-5);
- *Sécurité IT et confidentialité – Cadre pour la gestion de l'identité – Partie 1 : Terminologie et concepts* (ISO/IEC 24760-1);
- *Technologies de l'information – Techniques de sécurité – Vérification de l'identité* (ISO/IEC TS 29003).

Le Conseil Stratégique des DPI a publié des normes fondamentales sur la gouvernance des données et sur la confiance et l'identité numériques, comme la norme CAN/CIOSC 100-2:2020, *Gouvernance des données – Partie 2 : Accès de tiers aux données*, qui spécifie les exigences visant à protéger la sécurité des renseignements transmis à distance à des tiers. Parmi ses normes en cours d'élaboration, mentionnons CAN/CIOSC 100-7, *Gouvernance des données – Partie 7 : Gérance responsable des données*, qui spécifie les exigences minimales en matière de gouvernance des fiducies, de responsabilité et de gestion de la collecte et de l'échange de données. L'organisme travaille également sur des normes portant précisément sur les identifiants numériques – *Confiance et identité numérique – Partie 3 : Justificatifs d'identité numériques* – et les portefeuilles numériques – *Confiance et identité numérique – Partie 4 : Portefeuilles numériques* (CAN/CIOSC 103-4) – qui font partie d'une série de quatre normes sur la confiance et l'identité numérique, dont seule la première (CAN/CIOSC 103-1) a été publiée. L'un des comités techniques de l'organisme, qui se consacre à la confiance et à l'identité numériques, travaille présentement sur ces normes. En tant qu'OEN accrédité par le CCN, le Conseil Stratégique des DPI a publié quatre Normes nationales du Canada.

Hors du système de normalisation volontaire traditionnel, de nombreuses organisations actives dans le domaine des identifiants numériques ou de l'identité numérique ont également publié des normes, rapports techniques, documents d'orientation ou autres. Par exemple, le document de travail du W3C, *Decentralized Identifiers (DIDs) v1.0* est accessible sur GitHub et toute partie intéressée peut se créer un compte sur la plateforme afin de participer aux discussions l'entourant et à son élaboration. D'autres organisations rassemblent d'importants acteurs et défenseurs de l'industrie qui font progresser l'identité numérique, les identifiants numériques ou les technologies connexes. Au Canada, le Cadre de confiance pancanadien favorise la collaboration des secteurs privé et public pour la protection des identités numériques en ligne par des processus et pratiques normalisés dans l'ensemble de l'écosystème, et renforce la confiance envers les services numériques en prônant une prestation modernisée[81]. Ce cadre consiste en une suite de documents vérifiables de type normatif, fruit d'une collaboration entre le CCIAN, un forum neutre sans but lucratif, et le sous-comité de la gestion de l'identité des conseils mixtes, formés du Conseil de la prestation des services du secteur public et du Conseil des dirigeants principaux de l'information du secteur public.

81 CCIAN. Le Cadre de confiance pancanadien. https://diacc.ca/2016/08/11/pctf-overview/.

Pensons également au travail de la fondation OpenID, un organisme d'intérêt public sans but lucratif qui représente la communauté des développeurs, fournisseurs et utilisateurs de technologies d'identité. Plusieurs normes sont en cours d'élaboration, notamment dans ses groupes de travail sur les API financières qui travaillent sur un profil de sécurité[82].

L'initiative Kantara, une société constituée aux États-Unis et en Union européenne, a élaboré une norme sectorielle sur la réception du consentement[83]. L'initiative a également collaboré à l'international avec l'ISO, dans le comité ISO/IEC JTC 1/SC 27, Sécurité de l'information, cybersécurité et protection de la vie privée. Il y a également la Decentralized Identity Foundation, un groupe mondial d'entreprises qui fait la promotion de solutions d'identité décentralisées pour donner aux entités le contrôle de leur identité et permettre des interactions fiables. La fondation favorise les discussions sectorielles, contribue au code source ouvert et appuie l'interopérabilité.

En outre, FIDO Alliance, Internet Society, Hyperledger et OASIS ont également publié des normes de consortiums pertinentes. Comme il ne s'agit pas d'OEN accrédités, leurs publications ne sont pas reconnues dans le système de normalisation officiel, sauf si l'entreprise a demandé la collaboration d'un OEN accrédité, comme l'a fait OASIS auprès de l'organisme de normalisation américain ANSI, notamment, dans le cadre de l'élaboration de normes mondiales à l'ISO. L'organisation participe présentement aux comités ISO/PC 317, Protection des consommateurs : respect de la vie privée assuré dès la conception des biens de consommation et services aux consommateurs, et ISO/TC 324, Économie du partage. Sans avoir d'approche empirique pour mesurer le taux d'adoption de ces publications, le CCN estime que ces organisations recueillent une adhésion importante, vu le nombre et d'entreprises membres et leur influence, un bon indicateur de l'étendue de leur portée et de leurs retombées. Parmi les entreprises membres figurent plusieurs multinationales : Amazon, Apple, Bank of America, Facebook, Google, Microsoft, Visa, Nokia, IBM, Cisco, Dell, Huawei, Red Hat, TELUS et Walmart, entre autres[84],[85],[86],[87].

Aucun des grands OEN n'a publié de normes sur le système bancaire ouvert. Toutefois, le groupe d'entreprises américain FDX, qui a récemment étendu ses activités au Canada, a publié une norme sur l'utilisation d'API pour le partage des données des clients dans un système bancaire ouvert[88]. FDX et OBIC ont tous deux collaboré avec le Conseil stratégique des DPI, un OEN accrédité par le CCN. En 2020, dans le cadre de ce partenariat, le CSDPI a entrepris d'élaborer une série de normes nationales sur le système bancaire ouvert (CAN/CIOSC 110-x)[89].

Il importera également d'examiner le travail fait à l'international par des pays qui disposent déjà de systèmes bancaires ouverts, notamment l'initiative de système bancaire ouvert du Royaume-Uni (OBIE), la Directive sur les services de paiement 2 (DPS 2), la Singapore Financial Data Exchange (SGFinDex) et la loi australienne sur les droits des consommateurs par rapport à leurs données pour analyser les approches adoptées par d'autres pays et en tirer des pratiques exemplaires applicables au Canada.

De manière plus générale, les organismes de normalisation internationaux n'ont peut-être pas publié de normes sur le système bancaire ouvert, mais ils ont publié diverses normes touchant au système financier et à la sécurité qui sont à considérer dans un cadre de système bancaire ouvert. Par exemple, le comité technique de l'ISO sur les services financiers (ISO/TC 68) a publié les normes suivantes :

- *Services financiers – Gestion et sécurité du numéro personnel d'identification (PIN) – Partie 1 : Principes de base et exigences relatifs aux PINs dans les systèmes à carte* (ISO 9564:2017), parties 1, 2 et 4;
- *Banque – Gestion de clés (services aux particuliers)* (ISO 11568:2005), parties 1, 2 et 4;
- *Opérations bancaires de base – Services financiers mobiles* (ISO 12812:2017), parties 1 à 5;
- *Services financiers – Schéma universel de messages pour l'industrie financière* (ISO 20022), parties 1 à 8;
- *Services financiers – Prestataires de services de paiement tiers* (ISO/TR 21941:2017).

82 OpenID Foundation. « What is the Financial-grade API (FAPI) WG? » https://openid.net/wg/fapi/.
83 Kantara Initiative. « Kantara Initiative Releases the First Open, Global Consent Receipt Specification; Meets GDPR Requirements, Free For Download ». https://kantarainitiative.org/kantara-initiative-releases-first-open-global-consent-receipt-specification/.
84 FIDO Alliance. « FIDO Members ». https://fidoalliance.org/members/.
85 Internet Society. « Our Organization Members ». https://www.internetsociety.org/about-internet-society/organization-members/list/.
86 Hyperledger. « Members ». https://www.hyperledger.org/about/members.
87 OASIS Open. « Members ». https://www.oasis-open.org/member-roster/.
88 Financial Data Exchange. « Financial Data Exchange Releases New Open Finance Standards & FDX API Version 4.5 ». https://financialdataexchange.org/FDX/News/Press-Releases/FDX_Launches_Open_Finance_Standards_And_FDX_API_4.5.aspx.
89 Financial Post. « CIO Strategy Council Advances National Standards for Consumer Directed Finance ». https://financialpost.com/globe-newswire/cio-strategy-council-advances-national-standards-for-consumer-directed-finance.

Cas d'usage n° 3 – Responsabilisation et sécurité des consommateurs : chaînes d'approvisionnement numériques en alimentation

Contexte

Étant donné la complexité des chaînes d'approvisionnement alimentaires mondialisées, des technologies de traitement, des fraudes alimentaires et du commerce international, l'information concernant les chaînes d'approvisionnement alimentaires n'a jamais eu une si grande importance pour la sécurité, l'intégrité et la valeur des aliments consommés et produits au Canada.

On observe actuellement un virage numérique des chaînes d'approvisionnement dans l'agroalimentaire et l'agriculture. Dans une chaîne d'approvisionnement numérique, la série d'activités connexes (p. ex. transfert des matières premières, des biens et des pièces des mains du fournisseur à celles du consommateur) ainsi que les fonds, le matériel et les renseignements afférents reposent sur des technologies numériques.

Ces avancées constituent une occasion de donner aux consommateurs, aux gouvernements et à l'industrie les moyens nécessaires pour mettre à profit les données. À condition d'être transparentes et d'inspirer confiance, les technologies numériques pourraient accélérer les processus décisionnels et favoriser la santé, la sécurité et la rentabilité. La normalisation de la gouvernance de données en matière de chaînes d'approvisionnement permettrait aux consommateurs de faire des choix éclairés pour leur famille, aux gouvernements d'assurer une meilleure surveillance, à l'industrie de garantir la qualité de ses produits et aux chaînes d'approvisionnement de réagir plus rapidement pour contrer les risques.

Séances de discussion sur la responsabilisation et la sécurité des consommateurs dans les chaînes d'approvisionnement numériques en alimentation

Les 19, 20 et 21 janvier 2021, le Conseil canadien des normes (CCN) et le Collectif canadien de normalisation en matière de gouvernance des données ont animé des séances de discussion (deux étaient en anglais et une en français) avec le public et les intervenants sur la responsabilisation et la sécurité des consommateurs dans les chaînes d'approvisionnement numériques en alimentation. Une quarantaine de participants provenant de partout au pays y ont assisté, notamment des représentants de l'agriculture, de l'agroalimentaire et des technologies, ainsi que d'organismes gouvernementaux et de réglementation.

Au début de chaque séance, les représentants du CCN ont effectué une courte présentation sur le rôle du Collectif et l'importance des normes. Ensuite, un représentant de l'Agence canadienne d'inspection des aliments (ACIA) a fait un survol de l'état actuel du virage numérique des chaînes d'approvisionnement alimentaires ainsi que de la réglementation et de la *Loi sur la salubrité des aliments au Canada*. Les participants ont enfin été invités à s'exprimer sur les deux grands thèmes suivants :

- l'état actuel des chaînes d'approvisionnement numériques en alimentation au Canada, notamment les défis, les possibilités, les règles et les normes;
- l'avenir idéal, des avantages souhaités pour les consommateurs aux lois et règles nécessaires à l'établissement d'un cadre efficace pour les chaînes d'approvisionnement numériques en alimentation.

ÉTAT DES LIEUX ET DÉFIS ACTUELS

À l'occasion d'un exercice d'introduction interactif autour d'un tableau blanc, les participants ont été invités à se prononcer sur les défis auxquels sont confrontées les chaînes d'approvisionnement numériques en alimentation. Trois thèmes généraux et récurrents sont ressortis :

1. l'absence d'une proposition de valeur claire pour encourager l'adhésion et la participation des intervenants des chaînes d'approvisionnement;
2. l'existence d'un cloisonnement des données et le besoin de plateformes communes ou interopérables pour le transfert de données provenant de nombreuses sources;
3. la transparence et le besoin de nouveaux jeux de données améliorés pour faciliter la traçabilité des aliments.

Au terme de l'exercice, les participants ont échangé en petits groupes. Sur la question de l'état actuel des chaînes d'approvisionnement numériques en alimentation au Canada, ils sont majoritairement arrivés à la conclusion qu'une transparence et une traçabilité accrues étaient nécessaires pour favoriser la confiance des consommateurs et renforcer leur sécurité. Ils ont également mis en évidence des lacunes persistantes en matière de traçabilité des aliments et avancé que le temps et les ressources investis dans les efforts de traçabilité pour améliorer la qualité et l'étendue des données accessibles ne suffisaient pas. Enfin, conscients des défis que posent la diversité et la complexité de l'industrie, les participants ont souligné la nécessité de garantir l'interopérabilité des outils et des plateformes des chaînes d'approvisionnement numériques entre les secteurs et les administrations.

AVENIR IDÉAL

Dans leur réflexion sur l'avenir souhaité des chaînes d'approvisionnement numériques en alimentation au Canada, les participants ont évoqué la nécessité d'établir des mesures incitatives et des approches pratiques pour favoriser la participation. Ils ont convenu que le système doit faciliter l'adoption et l'accès aux données pour tous les acteurs de la chaîne de valeur et faire en sorte de responsabiliser chacun d'eux afin d'assurer la traçabilité et de prévenir la perte de données le long de la chaîne. Par ailleurs, plusieurs participants ont souligné le besoin de mesures incitatives ou de mécanismes de recouvrement des coûts pour encourager les acteurs de la chaîne de valeur à adhérer et à participer aux chaînes d'approvisionnement numériques. Finalement, le groupe a défini les principaux résultats souhaités de la normalisation des chaînes d'approvisionnement numériques en alimentation : interopérabilité, confidentialité et sécurité.

DISCUSSIONS

État des lieux des chaînes d'approvisionnement numériques en alimentation

Dans la première moitié des discussions en petits groupes, les participants ont été invités à donner leur opinion sur l'état des lieux des chaînes d'approvisionnement numériques en alimentation au Canada.

Voici les thèmes récurrents et les principales observations qui en sont ressortis.

Q1.1 : Quel est l'état des lieux des chaînes d'approvisionnement numériques en alimentation au Canada?

Thème n° 1 : La confiance et la sécurité des consommateurs dépendent d'une meilleure transparence et traçabilité.

Dans leur réflexion sur l'état des lieux des chaînes d'approvisionnement numériques en alimentation au Canada, plusieurs participants ont souligné le besoin d'améliorer la confiance et la sécurité des consommateurs, ainsi que l'importance de rendre l'information plus accessible pour que chacun puisse prendre des décisions éclairées dans le choix de ses aliments. Ils ont avancé que les consommateurs n'ont pas tous la même perception de la sécurité des aliments : si certains sont plutôt naïfs quant aux produits qu'ils achètent, tenant pour acquis que la sécurité de tout ce qui se trouve à l'épicerie a été vérifiée, d'autres se posent davantage de questions et ont de plus grandes attentes concernant l'origine des aliments, la méthode de production et les acteurs de la chaîne de valeur.

Ce sujet a soulevé plusieurs questions chez les participants, notamment les suivantes :

- De quelles informations les consommateurs ont-ils besoin, et lesquelles leur sont fournies actuellement?
- Quels sont les principaux obstacles à surmonter pour fournir ces informations aux consommateurs?

Lors des discussions sur la confiance et la sécurité des consommateurs, les participants sont globalement arrivés à la conclusion qu'une transparence et une traçabilité accrues étaient nécessaires. En outre, même s'ils estiment que fournisseurs et producteurs démontrent une volonté grandissante de mieux informer les consommateurs sur les ingrédients et les pratiques de production, ils ont aussi fait valoir que l'industrie aurait besoin d'un incitatif clair pour le faire systématiquement.

Les participants ont également mis en évidence des lacunes persistantes dans la traçabilité des aliments, insistant sur la nécessité de mieux suivre les aliments d'un bout à l'autre de la chaîne d'approvisionnement. Selon eux, le temps et les ressources actuellement investis dans les efforts de traçabilité ne suffisent pas pour améliorer la qualité et l'étendue des données accessibles. Pour certains, une norme commune sur la traçabilité pourrait stimuler l'innovation et la mise en commun de l'information.

PROBLÈMES DE NORMALISATION

- Le système actuel n'est pas nécessairement accessible à tous. Par exemple, de nombreux fournisseurs n'ont pas l'infrastructure technologique requise pour contribuer à ce type de système de données.
- Il est actuellement difficile pour les consommateurs d'obtenir de l'information sur les aliments qu'ils consomment (p. ex. traçabilité). Les acteurs de la chaîne de valeur devraient être tenus responsables de rendre les données plus accessibles.

Thème n° 2 : Dans une industrie complexe et diversifiée, la coopération, l'interopérabilité et l'accessibilité sont des facteurs de succès déterminants.

Les participants ont souligné la diversité et la complexité de l'agroalimentaire et de l'agriculture, mentionnant les différences considérables entre les secteurs et les administrations au Canada et à l'international. Ils ont expliqué que les chaînes d'approvisionnement varient fortement d'un type de produits à l'autre (produits laitiers, poulet, œufs, fruits et légumes, etc.). Parmi les différences : la façon de mettre en place les cadres des chaînes d'approvisionnement numériques. Certains participants ont d'ailleurs dénoncé le fait que, malgré les quelques efforts isolés, l'industrie ne disposait d'aucune norme uniforme en ce sens.

Compte tenu de ces différences et des défis grandissants que pose la salubrité des aliments, les participants ont souligné le besoin de garantir l'interopérabilité des outils et des plateformes des chaînes d'approvisionnement numériques entre les secteurs et les administrations. Le groupe a aussi mentionné que plusieurs collectes de données sont en cours, mais que les producteurs n'ont pas les connaissances ou les compétences techniques pour rassembler ces données et les diffuser dans toute la chaîne de valeur. Les participants ont même avancé que plusieurs fournisseurs ne possèdent pas nécessairement la technologie requise pour contribuer à un tel système de données. Il faudra donc veiller à ce qu'il soit adaptable et accessible à tous.

Fait intéressant, certains participants ont indiqué que la pandémie avait nui à la collaboration dans l'industrie, l'un des participants affirmant que « la façon dont nous avions l'habitude de collaborer avant la pandémie de COVID-19 ne convient plus; nous devrons repartir à neuf et rééquilibrer le tout. L'équilibre n'y est plus. Les différences entre les chaînes d'approvisionnement sont majeures. Il faudrait entamer une nouvelle discussion sur ce que la santé publique fait et ce que nous devrions faire de notre côté. »

PROBLÈMES DE NORMALISATION

- Il n'existe pas de proposition de valeur claire. Les acteurs de la chaîne de valeur ne comprennent pas nécessairement l'importance de participer et de contribuer à un système d'approvisionnement alimentaire numérique intégré.
- Certains craignent que la numérisation fasse obstacle à l'interopérabilité et à la connectivité générale. Des mesures incitatives seront nécessaires pour opérer le virage numérique.
- Les habitudes de collaboration qui existaient dans les chaînes d'approvisionnement alimentaires avant la pandémie de COVID-19 ne conviennent plus.

Thème nº 3 : Un accès simplifié à l'information est essentiel pour les consommateurs.

Plusieurs participants ont affirmé que les consommateurs font preuve de plus en plus de discernement quant aux aliments qu'ils achètent et consomment. Toutefois, il n'existe pas de démarche standard et simple pour se renseigner sur l'origine et les méthodes de production de ce qui se retrouve dans son assiette. Un participant a proposé l'utilisation de codes QR balayables comme solution, mais il faudrait établir des normes pour garantir une application cohérente et l'accessibilité des données aux consommateurs.

PROBLÈMES DE NORMALISATION

- Il est actuellement difficile pour les consommateurs d'obtenir de l'information sur les aliments qu'ils consomment (p. ex. traçabilité). Les acteurs de la chaîne de valeur devraient être tenus responsables de rendre les données plus accessibles.

Q1.2 : À votre connaissance, quels sont les règles, les règlements et les normes qui encadrent actuellement les chaînes d'approvisionnement numériques en alimentation?

Thème nº 4 : Le Canada pourrait se baser sur les normes et les déploiements technologiques précurseurs réussis qui existent déjà.

Les participants ont relevé plusieurs normes existantes d'intérêt pour les chaînes d'approvisionnement numériques en alimentation, notamment les suivantes :

- Certification AG Data Transparent (États-Unis)
- Plateforme de certification des semences de l'ACIA à l'appui de la *Loi* et du *Règlement sur les semences*
- Cadre de la DAMA (présentation, données unifiées)
- Études du Groupe CSA sur les normes pertinentes, plus particulièrement le rapport *Provenance and Traceability of Rare Earth Products*

Ils ont également mentionné pendant les discussions plusieurs déploiements technologiques précurseurs réussis qui pourraient aider à l'élaboration de futures normes, notamment les suivants :

- Dans le cadre du Programme canadien des priorités stratégiques de l'agriculture, Agriculture et Agroalimentaire Canada a investi dans un projet pilote inédit qui utilise des chaînes de blocs pour suivre les semences de soya locales certifiées, de la production aux étagères des épiceries, en passant par la transformation.
- IBM Food Trust[MC] est la première solution de chaînes de blocs dédiée à la salubrité des aliments qui permet aux partenaires commerciaux d'échanger de l'information sur les aliments en toute confiance et sécurité, créant ainsi une chaîne d'approvisionnement alimentaire mondiale plus transparente et fiable.
- Microsoft a mis au point FarmBeats, une technologie qui combine chaînes de blocs, drones et intelligence artificielle pour améliorer la productivité et réduire la consommation d'eau des exploitations agricoles.

Avenir des chaînes d'approvisionnement numériques en alimentation

Dans la seconde moitié des **discussions en petits groupes**, les participants ont été invités à donner leur opinion sur l'avenir souhaité des chaînes d'approvisionnement numériques en alimentation au Canada.

Voici les thèmes récurrents et les principales observations qui en sont ressortis.

Q2.1 : Quel est l'avenir idéal des chaînes d'approvisionnement numériques en alimentation au Canada?

Thème n° 5 : Un cadre pragmatique et axé sur la valeur est nécessaire à l'adhésion et à la participation de tous les acteurs des chaînes d'approvisionnement.

Dans leur réflexion sur l'élaboration des chaînes d'approvisionnement numériques en alimentation, les participants ont souligné la nécessité d'établir des mesures incitatives et des approches pratiques pour favoriser la participation.

Lors de la discussion, certains ont suggéré qu'un cadre pragmatique serve de principe directeur pour les chaînes d'approvisionnement numériques en alimentation au Canada. Ils ont expliqué que l'approche ne devait pas exiger un processus laborieux ou une mise en œuvre ambitieuse, pour éviter de paralyser les consommateurs et les industries. Selon un participant, par exemple, si la réglementation est trop rigide ou stricte, il pourrait y avoir des conséquences imprévues sur ces deux groupes. Un autre a résumé sa vision de l'approche idéale : « dirigée par l'industrie et soutenue par le gouvernement ».

Les participants s'entendaient pour dire que le système doit faciliter l'adhésion et l'accès aux données pour tous les acteurs de la chaîne de valeur, et que chaque intervenant doit être tenu responsable de la traçabilité et de la préservation des données. Pour eux, le point de liaison entre les fermiers et les transformateurs est un maillon important de la chaîne d'approvisionnement où les obstacles de la numérisation restent à surmonter, car les chiffriers et les formulaires papier y sont encore souvent utilisés pour les échanges d'information.

Un autre principe organisationnel proposé par le groupe consistait à « trouver un avantage mutuel qui aurait une incidence collective ». C'est pourquoi plusieurs participants ont évoqué la nécessité de créer des mesures incitatives pour favoriser l'adhésion et la participation des acteurs de la chaîne de valeur aux chaînes d'approvisionnement numériques. L'un d'entre eux a proposé que les fermiers reçoivent un certain montant pour chaque animal d'élevage afin de pouvoir recouvrer les frais liés à la collecte et à la transmission des données. Un autre a suggéré que les consommateurs couvrent, par la voie d'une hausse des prix, les coûts associés aux renseignements supplémentaires sur l'origine des aliments et les méthodes de production utilisées, puisqu'ils ajoutent de la valeur aux produits.

Q2.2 : Quels sont les règles, les règlements et les normes nécessaires pour établir un cadre des chaînes d'approvisionnement numériques en alimentation au Canada?

Thème n° 6 : Les normes devraient être axées sur l'interopérabilité, la confidentialité et la sécurité.

Pour les participants, l'interopérabilité, la confidentialité et la sécurité sont les principaux résultats souhaités de la normalisation des chaînes d'approvisionnement numériques en alimentation.

Du point de vue de l'interopérabilité, le groupe a fait valoir que tous les acteurs de la chaîne d'approvisionnement (producteurs, détaillants et transformateurs) devraient être continuellement impliqués pour assurer l'uniformité. Selon un participant, « tous les intervenants doivent se rassembler pour examiner les cas d'usage, qui sont constamment en évolution et en expansion ». Certains autres ont exprimé le besoin de fixer des règles ou des règlements garantissant l'accessibilité des données via toutes sortes de systèmes, de technologies et de plateformes. C'est pourquoi l'élaboration de normes ouvertes sur les API a été suggérée.

La nécessité d'élaborer des politiques rigoureuses sur la confidentialité et la sécurité dans le stockage et le transfert de données a aussi été mise en lumière. Les participants trouvaient particulièrement important que tous les utilisateurs d'une technologie ou d'une application sachent comment et à qui leurs renseignements seront divulgués. L'un d'entre eux a d'ailleurs souligné les défis de mise en œuvre posés par les écarts dans la réglementation des différentes provinces sur la confidentialité et la sécurité, ainsi que par le besoin d'établir des normes internationales cohérentes.

Thème n° 7 : Les certifications de produits devraient être maintenues dans la transition vers les chaînes d'approvisionnement numériques en alimentation.

Les certifications de produits alimentaires ont été citées comme une pratique exemplaire pour la sensibilisation et l'information des consommateurs, qui devrait être maintenue dans la transition vers les chaînes d'approvisionnement numériques en alimentation. Les participants ont mentionné que ces certifications constituent pour les consommateurs une marque connue et éprouvée des caractéristiques et des garanties qu'ils recherchent, qu'il s'agisse du pays ou de la région d'origine, ou de normes environnementales, de production biologique ou autres.

Rapport du groupe de travail sur le cas d'usage

Le groupe de travail sur le cas d'usage a utilisé l'outil d'analyse du cycle de vie du Collectif pour isoler les lacunes et les enjeux de normalisation. À l'aide d'un schéma des flux de produits, il a établi la liste de tous les acteurs participant à la complexe chaîne d'approvisionnement (voir l'image à la fin du rapport). Plusieurs difficultés récurrentes ont été cernées et classées en trois thèmes.

Le groupe a conclu que les lacunes et les enjeux précédemment relevés par les quatre groupes de travail pouvaient s'appliquer au cas d'usage. Il a donc déterminé les principaux facteurs influençant les décisions des consommateurs et les a répartis selon neuf grands enjeux de gouvernance des données.

CONSTATS GÉNÉRAUX

Les chaînes d'approvisionnement alimentaires sont complexes (pratiques de gestion, sources d'approvisionnement, technologies de traitement, éclosions, commerce provincial et international, gestion et communication des données, systèmes d'assurance), et les consommateurs accordent de plus en plus d'importance aux gages de confiance et à la transparence; les renseignements sur les chaînes d'approvisionnement n'ont jamais été aussi intimement liés à la sécurité, à l'intégrité et à la valeur des aliments consommés et produits au Canada. C'est pourquoi on observe actuellement un virage numérique des chaînes d'approvisionnement dans l'agroalimentaire et l'agriculture.

Thèmes principaux :

- Numérisation et interopérabilité de l'industrie
- Besoins et unification en matière de données
- Accès, confidentialité et rôles relatifs aux données

1. **Thème no 1 – Numérisation et interopérabilité de l'industrie :** Si la numérisation de l'industrie est compliquée, c'est qu'il n'existe pas de proposition de valeur claire pour encourager les acteurs des chaînes d'approvisionnement à faire une analyse de rentabilité de la numérisation et de la traçabilité. Lors des consultations publiques, les discussions sur l'avenir idéal de l'industrie ont mis en lumière la nécessité d'offrir des mesures incitatives pour favoriser la participation aux chaînes d'approvisionnement numériques.
2. **Thème no 2 – Besoins et unification en matière de données :** Le groupe de travail sur le cas d'usage a fait valoir la nécessité d'unifier les données et d'augmenter l'interopérabilité pour favoriser les échanges d'information. Cette façon de procéder renforcerait la confiance des consommateurs en assurant la transparence et un accès facile aux renseignements qui influent sur les décisions d'achat. Les participants aux consultations publiques ont soulevé des points similaires concernant la confiance des consommateurs et l'amélioration de l'accès à l'information, de la traçabilité et de la transparence dans la chaîne d'approvisionnement.

   Cependant, l'unification pose un défi de taille : celui de la gestion collective d'une chaîne d'approvisionnement numérique. La chaîne actuelle souffre d'un cloisonnement des données. Il faudra établir des relations multilatérales et de nouveaux services visant de nouveaux acteurs (p. ex. les consommateurs), d'où l'utilité de solutions comme les chaînes de blocs.

3. **Thème no 3 – Accès, confidentialité et rôles relatifs aux données :** Les données actuellement collectées et stockées ne sont pas accessibles dans toute la chaîne d'approvisionnement, en raison d'un cloisonnement au point de collecte et d'une infrastructure technologique déficiente, en plus d'écarts dans la qualité des données et la production de rapports. En outre, l'accès aux données stockées est difficile pour les consommateurs.

   Il faut normaliser les principaux éléments de données à saisir et déterminer lesquels doivent être partagés. Il faut aussi normaliser les rôles relatifs aux données et les autorisations à l'égard de chaque transaction de la chaîne d'approvisionnement, et définir les engagements et les motivations des différents acteurs à des fins de reddition de comptes et de protection des renseignements commerciaux confidentiels.

CONSTATS DU GROUPE DE TRAVAIL

En transposant les enjeux soulevés par les quatre groupes de travail dans le contexte de la responsabilisation et de la sécurité des consommateurs, le groupe a isolé les grands enjeux suivants *(les constats sont regroupés par enjeu; l'enjeu principal est en gras)* :

1. **Enjeu 20 – Accès aux données :** Cet enjeu se rapporte au processus entourant l'accessibilité et la convivialité des données. Les consommateurs auront besoin d'un accès convivial à l'information pour prendre des décisions d'achat éclairées; la normalisation de cet accès leur assurera les outils nécessaires. Toutefois, l'application d'une approche de normalisation unique pourrait s'avérer peu avantageuse pour l'industrie. La définition des accès aux données devrait être confiée aux utilisateurs du système.
2. **Enjeu 11 – Collecte des données :** Cet enjeu vise principalement la collecte des données primaires. Avant de déterminer comment les données doivent être saisies et échangées pour assurer leur sécurité et leur fiabilité, il faudra d'abord comprendre la nature et l'utilité des mécanismes en place pour contrôler la qualité et l'intégrité dans la chaîne d'approvisionnement et les besoins en la matière. Si certains acteurs de la chaîne emploient les solutions de GS1, d'autres utilisent encore un système papier. Il s'agit d'un obstacle important à la numérisation qui devrait être pris en compte dans la création de normes sur la collecte des données.

3. **Enjeu 21 – Conservation des données :** Cet enjeu met en lumière le besoin de procédures de conservation des données normalisées au sein des organismes. Une fois un produit retiré définitivement des étagères, combien de temps doit-on conserver les données de traçabilité? Le groupe de travail sur le cas d'usage estime que la conservation et la tenue à jour des données devraient simplement faire l'objet de lignes directrices, car un cadre réglementaire serait trop rigide pour répondre à tous les besoins. (N.B. : Le *Règlement sur la salubrité des aliments au Canada* explique où conserver les documents de traçabilité et pour combien de temps.)
4. **Enjeu 22 – Gestion de l'identité :** Cet enjeu se rattache à la nécessité de normaliser les termes et les concepts relatifs à la gestion de l'identité pour garantir une interprétation uniforme. Il est important que la chaîne d'approvisionnement puisse avoir confiance en l'identité de tous les acteurs. Ainsi, il faudrait normaliser la gestion de chaque identité, les méthodes d'authentification et les autorisations, rôles et privilèges s'appliquant aux différents contextes. On note aussi le besoin d'employer des processus fiables pour déterminer quels acteurs fournissent des données à la chaîne d'approvisionnement et intégrer les nouveaux participants, afin de favoriser et d'améliorer la confiance et la transparence.
5. **Enjeu 13 – Visibilité des données :** Cet enjeu porte principalement sur les jeux de données existants et les façons de les trouver et de les utiliser. Il est important que les acteurs sachent où et comment chercher les données dont ils ont besoin. Bien que toute la chaîne d'approvisionnement contribue à la collecte d'information, les connaissances et les aptitudes techniques requises pour intégrer les données et les diffuser dans toute la chaîne de valeur demeurent lacunaires. Les consommateurs devraient être à même de concrètement chercher et obtenir des renseignements sur une exploitation agricole, un transformateur alimentaire ou autre.
6. **Enjeu 9 – Rôles des acteurs et des opérations en matière de traitement des données :** Cet enjeu explore les rôles des acteurs du traitement des données au long du cycle de vie de la chaîne d'approvisionnement et couvre l'entièreté du processus de gestion des données, de leur collecte à leur consommation. Compte tenu de la complexité de la chaîne d'approvisionnement alimentaire, il est crucial que les rôles des acteurs soient clairement définis. Pour assurer la responsabilisation de chacun, améliorer la traçabilité et prévenir la perte de données le long de la chaîne d'approvisionnement, il serait aussi important d'examiner le rôle des consommateurs et de reconnaître, en plus des acteurs habituels, tous les participants de la chaîne de valeur.
7. **Enjeu 16 – Gestion des métadonnées et enjeu 11 – Collecte des données :** La gestion des métadonnées est étroitement liée à la collecte des données; pour les besoins du présent rapport, ces deux enjeux ont été combinés. La gestion des métadonnées comprend la collecte, la gestion, l'accessibilité et la viabilité des métadonnées. Il serait primordial de définir le type de métadonnées (p. ex. type d'identifiants, format, système de codage) requis dans la chaîne d'approvisionnement pour faciliter l'utilisation des données. La normalisation des principes régissant les descripteurs de données faciliterait l'identification des intervenants qui collectent des données et renforcerait la transparence de leurs systèmes de gestion des données.
8. **Enjeu 28 – Transparence, parcours et traçabilité des données :** Cet enjeu se rapporte principalement à la transparence et à la traçabilité des données au cours de leur cycle de vie. La traçabilité est un défi de taille pour les chaînes d'approvisionnement numériques en alimentation au Canada. Pour combler les lacunes persistantes sur ce plan, il faudra d'abord comprendre comment les transferts de données sont enregistrés, qui peut consulter le parcours des données et quelle information est conservée. La normalisation des exigences minimales de collecte des données, de même que la normalisation des éléments et des attributs de données, permettrait aux consommateurs d'être mieux informés et aux producteurs de se distinguer sur le marché. Toute normalisation plus poussée de l'accès risquerait d'être trop restrictive et moins volontaire.
9. **Enjeu 29 – Portabilité et mobilité des données :** Cet enjeu est axé sur la capacité à échanger des données entre différents systèmes sans manipulations supplémentaires. Il faudrait déterminer quels acteurs de la chaîne d'approvisionnement peuvent demander une copie numérique de leurs données et établir des lignes directrices pour la suppression des données afin de préserver les échanges d'information entre les systèmes et de réduire la dépendance des exploitants agricoles et des producteurs à l'égard des fournisseurs de TI.

RECOMMANDATIONS

Suivant l'examen du cas d'usage et les consultations publiques, le groupe de travail propose que le Collectif établisse en priorité des normes pour les enjeux ci-dessous. Les recommandations sont propres au secteur alimentaire et ne s'appliquent pas à la gouvernance générale des données. Les enjeux marqués d'un numéro proviennent de la liste des 35 enjeux de gouvernance de données dressée par les quatre groupes de travail du Collectif.

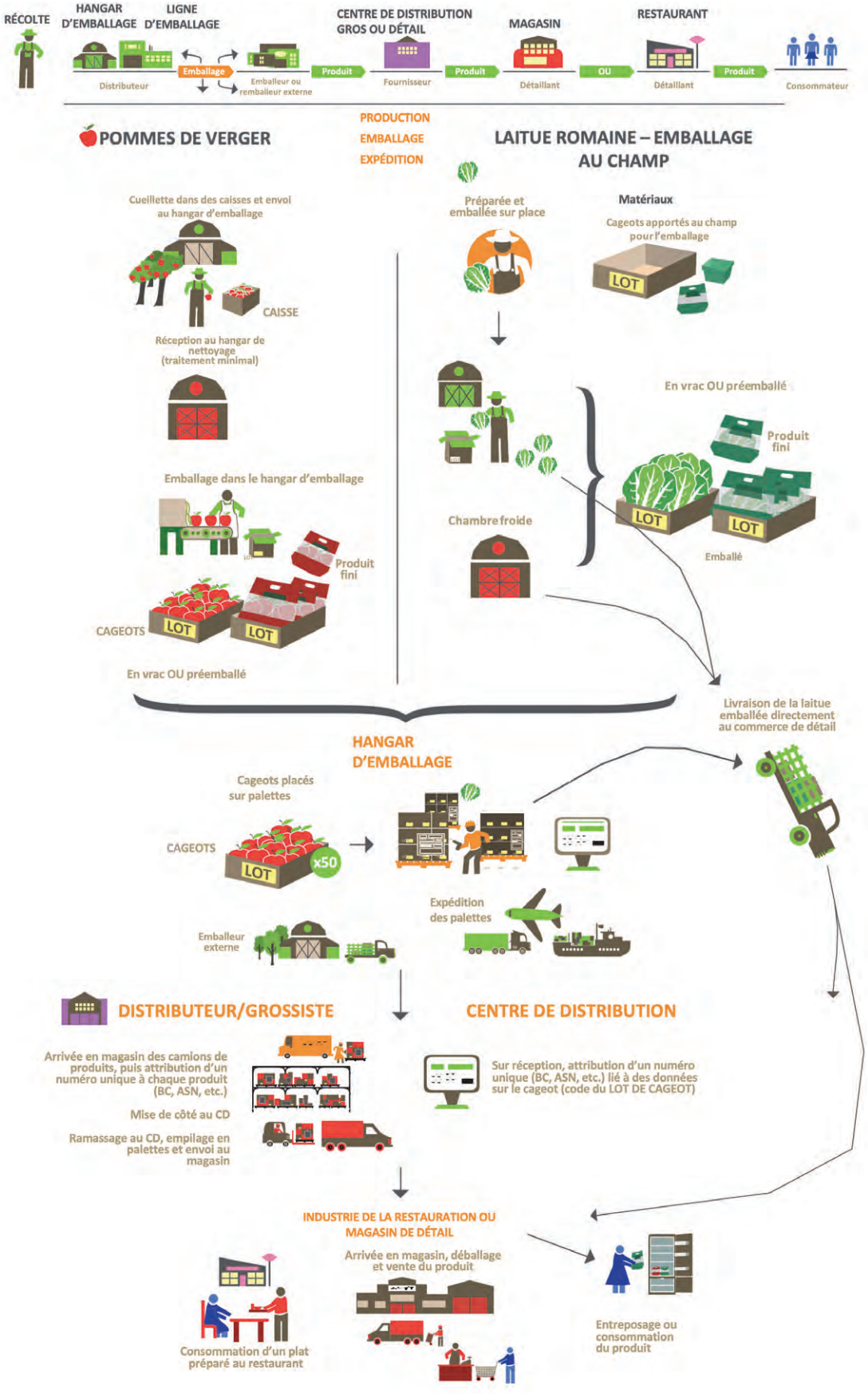
1. **Enjeu 20 – Accès aux données :** Il faudrait réaliser plus d'études pour s'assurer que la normalisation serait avantageuse pour le secteur de l'agroalimentaire et de l'agriculture. À noter que l'emploi d'une approche unique pour l'accès aux données par les tiers pourrait poser un problème d'interprétation dans les diverses filières. Les utilisateurs du système sont peut-être les mieux placés pour définir les accès.
2. **Enjeu 21 – Conservation des données :** Les lignes directrices seront ici à préférer aux règles strictes dans la normalisation des pratiques de conservation et d'entretien des données dans la chaîne d'approvisionnement.
3. **Enjeu 22 – Gestion de l'identité :** La normalisation des méthodes d'authentification permettrait de garantir l'authenticité de l'identité des différents acteurs de la chaîne d'approvisionnement.
4. **Enjeu 13 – Visibilité des données :** Il serait important de normaliser les processus de recherche des données pour que les consommateurs et les autres acteurs de la chaîne d'approvisionnement puissent facilement trouver l'information dont ils ont besoin.
5. **Enjeu 9 – Rôles des acteurs et des opérations en matière de traitement des données :** La normalisation des rôles assurerait la responsabilisation de chacun dans l'amélioration de la traçabilité et la prévention des pertes de données le long de la chaîne d'approvisionnement
6. **Enjeu 16 – Gestion des métadonnées :** La normalisation des principes régissant les descripteurs de données faciliterait l'identification des intervenants qui collectent des données et renforcerait la transparence de leurs systèmes de gestion des données.
7. **Enjeu 28 – Transparence, parcours et traçabilité des données :** La normalisation des exigences minimales de collecte des données, de même que la normalisation des éléments et des attributs de données, est cruciale. Toutefois, une normalisation plus poussée de l'accès risquerait d'être trop restrictive et moins volontaire. Il serait aussi important d'étudier les normes de traçabilité existantes, par exemple la Norme de traçabilité de GS1 Global et les normes de traçabilité de l'ISO (plus précisément ISO 22005, *Traçabilité de la chaîne alimentaire – Principes généraux et exigences fondamentales s'appliquant à la conception du système et à sa mise en œuvre*). Ces normes sont utilisées dans bon nombre de chaînes d'approvisionnement et devraient être examinées par le Collectif.
8. La normalisation des chaînes d'approvisionnement numériques en alimentation devrait viser principalement l'interopérabilité, la confidentialité et la sécurité.

OBSERVATIONS FINALES

La diversité et la complexité de la chaîne de valeur agroalimentaire et agricole compliquent la normalisation. Cette dernière aurait plusieurs avantages : assurer la qualité des produits, réduire et atténuer les risques (p. ex. en cas d'éclosion), et permettre aux consommateurs de prendre des décisions éclairées. Malgré cela, l'industrie se montre réticente face à l'adoption de règles et de formulations ayant des visées de réglementation plutôt que d'orientation, ce qui pourrait ralentir l'innovation et avoir des conséquences indésirables pour le secteur. Il faudrait donc tenter d'éviter, dans l'élaboration de nouvelles normes de gouvernance des données, les mises en œuvre trop ambitieuses et les processus trop complexes pour ne pas paralyser les consommateurs ou les entreprises.

Le groupe de travail sur le cas d'usage est reconnaissant d'avoir pu réaliser cet examen. Il s'est inspiré des commentaires recueillis lors des consultations publiques pour formuler les recommandations qu'il soumet au Collectif. Ses membres demeurent à disposition pour répondre aux questions et aux commentaires, s'il y a lieu.

Schéma de traçabilité des flux de produits – Créé par l'Agence canadienne du pari mutuel



Cas d'usage prospectif sur la surveillance des enfants et les systèmes d'apprentissage numérique

Contexte

Alors que les consultations sur les trois cas d'usage touchaient à leur fin en janvier 2021, le Collectif canadien de normalisation en matière de gouvernance des données a commencé à recevoir des suggestions de cas d'usage pour une deuxième version de la feuille de route. L'un des cas proposés portait sur la surveillance des enfants et les systèmes d'apprentissage numérique et soulignait l'importance de poursuivre les discussions transversales sur la gouvernance des données et ses effets sur différents secteurs. Pour évaluer ce sujet prioritaire, le Conseil canadien des normes (CCN) s'est allié à Hill+Knowlton Stratégies pour organiser une séance de discussion de deux heures.

Durant cette séance, le CCN et les participants ont pu se renseigner sur les opinions de la population canadienne et le travail actuellement en cours dans le domaine. Les réflexions se sont articulées autour de deux grands thèmes. Il a d'abord été question de l'état des lieux de la surveillance en ligne au pays et de son encadrement normatif :

- Quels défis pose actuellement la gouvernance des technologies par rapport à la surveillance numérique? (Quelles sont les informations nécessaires, sont-elles bien protégées, et qui peut les consulter?)
- Quels règlements, règles ou normes sont en place, à votre connaissance, pour encadrer la surveillance numérique?

Ensuite, les réflexions ont été orientées sur l'avenir de l'encadrement des technologies et de la surveillance en ligne :

- Quel est l'avenir idéal de la surveillance numérique au Canada? (Quelles sont les avenues idéales, et quels avantages présente la montée en puissance de la surveillance en ligne?)
- Quelles sont les répercussions sur le consentement parental de la nouvelle version de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et des normes émergentes de gouvernance des données?
- Quels sont les règlements, les règles ou les normes nécessaires pour encadrer la gouvernance des technologies et la surveillance en ligne au Canada?

De nos jours, pandémie oblige, les interactions en personne sont limitées, et les secteurs d'activités et organismes traditionnels ont eu très peu de temps pour se restructurer et s'adapter à la réalité de la concurrence numérique. La crise sanitaire a fait ressortir les lacunes de la surveillance en ligne, question particulièrement importante à l'heure où les élèves du Canada utilisent de plus en plus les systèmes d'apprentissage numérique.

Un manque de normes sur la gouvernance des données, le non-respect des règlements protégeant la confidentialité et une mise en œuvre incohérente des procédures opérationnelles et de sécurité dans les écoles : voilà les risques qui menacent les enfants, les parents et le tissu social du pays. Par ailleurs, les différentes perceptions culturelles des provinces vis-à-vis de la protection de la vie privée entraînent de grands risques de cybersécurité.

La transition des écoles vers des systèmes d'apprentissage numérique en contexte pandémique a projeté ces problèmes au premier plan, suscitant de sérieuses préoccupations quant à l'encadrement des risques relatifs à l'identité numérique et à la vulnérabilité des écoles, du corps enseignant, des parents et des élèves.

Les technologies de l'éducation posent depuis longtemps des problèmes de confidentialité et d'équité. La pandémie ayant entraîné la multiplication de ces technologies et des systèmes d'apprentissage numérique, il faut maintenant élaborer des initiatives et des procédures opérationnelles communes pour encadrer la surveillance numérique et limiter les principaux risques entourant l'identité numérique, la sécurité et la confidentialité. Les écoles ne saisissent pas toujours pleinement la portée de ces risques, par exemple la vente des données des élèves à des acteurs externes à des fins de marketing, la surveillance des activités scolaires et parascolaires et la perte d'autonomie des élèves constamment surveillés. La surveillance en ligne dans le cadre de systèmes d'apprentissage numérique doit être une priorité pour les instances, les acteurs politiques et les chefs d'entreprise. Ceux-ci doivent porter le sujet à l'attention des pouvoirs publics pour résoudre les problèmes qui pèsent sur les réseaux numériques et assurer la prise en compte des individus de toutes les communautés du Canada.

Si le pays, les provinces et les conseils scolaires ont défini des politiques claires, leur application dans les écoles présente des lacunes. Par exemple, dans le secteur ontarien de l'éducation, il existe une politique sur la gouvernance des données visant les renseignements que détiennent les écoles de la province, mais les fournisseurs de services tiers en sont exemptés. Dès lors, bon nombre d'applications ne sont pas examinées ou contrôlées au préalable. Souvent, les administrateurs scolaires ne vérifient pas la conformité des technologies de l'éducation aux normes de confidentialité, ce qui peut mener à des affirmations trompeuses sur la protection de la vie privée. À cela s'ajoute l'application inégale des politiques de cybersécurité et de sécurité physique dans les écoles. Résultat : un système d'éducation dans lequel les enfants sont vulnérables, les parents ne connaissent pas les dangers, les enseignants sont pressés d'offrir des programmes efficaces utilisant des applications dont ils ne comprennent pas les répercussions, et les administrateurs des TI sont en nombre insuffisant pour voir au respect des politiques. Le Canada présente d'importantes variations régionales sur le plan du déploiement des technologies de l'éducation dans les systèmes scolaires de la maternelle à la 12e année, lesquelles ont entraîné l'utilisation de plateformes et de services (p. ex. Zoom et Skype) qui n'ont pas été conçus à des fins éducatives et qui recueillent souvent beaucoup de renseignements personnels sur les élèves (p. ex. nom, école et utilisation faite de la plateforme), constituant ainsi un danger à long terme pour la vie privée et l'autonomie.

De plus, la recherche à ce sujet indique que la majorité des entreprises de technologies de l'éducation n'informent pas les parents des risques et ne recueillent donc pas un consentement éclairé. En outre, leurs mesures de sécurité des données, de transparence et de protection des identifiants d'apprentissage numérique (métadonnées) ne satisfont pas au septième principe de la LPRPDE sur les mesures de sécurité et les avis de risque et de consentement clairs.

Il s'agit d'un problème pour la population canadienne, car les plateformes d'apprentissage numérique et les entreprises de technologies de l'éducation n'exigent pas le consentement éclairé des parents et ne suivent pas de pratiques exemplaires pour le consentement à deux facteurs (soit les avis de risque et l'avis de consentement). Les parents ne sont ainsi pas à même de reconnaître les risques que la collecte et l'utilisation des données posent pour leurs enfants. Il est primordial que les plateformes et les technologies de l'éducation se conforment aux pratiques exemplaires de l'industrie, notamment le consentement à deux facteurs, et obtiennent le consentement parental légal. Ces préoccupations sont particulièrement manifestes sur le plan de la sécurité des renseignements personnels : en effet, seulement un cinquième des technologies affichent des politiques de sécurité et de protection des données adaptées au contexte canadien.

Avec la transition du secteur de l'éducation vers les plateformes numériques et les autres outils virtuels d'apprentissage en classe, il faut évaluer les risques que ces technologies présentent pour les enfants vulnérables. Pratiquement aucune des technologies et applications d'apprentissage numérique ne comporte de mesures adéquates de protection contre la surveillance en ligne et les dangers pour l'identité numérique des écoles, des enseignants, des élèves et des parents. Il est crucial d'assurer la cohérence entre les politiques et les procédures opérationnelles visant les technologies de l'éducation et des médias sociaux au pays, non seulement pour les parents, mais aussi pour la société tout entière.

L'utilisation de métadonnées canadiennes sans consentement dénote que les fournisseurs de services ont profilé les données des citoyens et les ont agrégées afin de créer des produits pour les médias sociaux, et ce, sans protections. Le fait d'agréger des données pour créer des produits qui donnent accès à ces mêmes données contrevient aux lois sur la protection de la vie privée du Canada, et va à l'encontre de la culture et des attentes de sa population.

Il est impératif de protéger les métadonnées d'apprentissage numérique des enfants pour réduire les risques importants que posent certains facteurs comme l'inégalité des formations, le manque d'uniformité dans les politiques des écoles et des conseils scolaires, l'application déficiente des politiques et des recommandations existantes, et la disparité des politiques du fédéral, des fournisseurs de services et des exploitants.

Compte tenu de ces défis, la normalisation sera nécessaire pour établir des cadres de consentement à la surveillance en ligne qui respectent les valeurs canadiennes et répondent aux besoins des enfants qui y sont exposés. Ce nouveau cas d'usage potentiel sur la gouvernance des données favoriserait l'application des pratiques exemplaires en matière de prestation de services de cybersécurité et de sécurité physique, ainsi que des mesures d'intervention essentielles à un avenir numérique au Canada.

SÉANCE DE DISCUSSION SUR LA SURVEILLANCE DES ENFANTS ET LES SYSTÈMES D'APPRENTISSAGE NUMÉRIQUE

Le 25 février 2021, le CCN a organisé une séance de discussion avec 23 participants pour connaître l'opinion des Canadiens et des Canadiennes au sujet de la surveillance des enfants et des systèmes d'apprentissage numérique et se renseigner sur le travail actuellement en cours dans le domaine. Animée par Hill+Knowlton Stratégies, la séance a débuté par un exercice autour d'un tableau blanc visant à mieux comprendre les enjeux principaux. Ont suivi deux périodes de discussion, d'abord sur la situation actuelle au Canada, puis sur l'avenir idéal.

État des lieux de la surveillance des enfants et des systèmes d'apprentissage numérique

Dans la première moitié de la discussion, les participants ont été invités à donner leur opinion sur l'état actuel de la surveillance des enfants et des systèmes d'apprentissage numérique.

Q1.1 : Quels défis pose actuellement la gouvernance des technologies par rapport à la surveillance en ligne? (Quelles sont les informations nécessaires, sont-elles bien protégées, et qui peut les consulter?)

Thème nº 1 : Définitions

Les participants ont convenu de définir clairement la surveillance en ligne pour éviter les divergences d'interprétation. Ils ont aussi souligné l'importance de comprendre la différence entre la surveillance et la collecte de données. Le premier concept se rapporte généralement à la surveillance de l'utilisation des appareils et des données ainsi que des occupations d'une personne à partir de son activité en ligne, souvent de manière non réglementée et sans consentement. Mais si la technologie peut mener à une surveillance, il ne faut pas confondre cette dernière avec la collecte légale de données (p. ex. numéros et noms des élèves et renseignements sur les cours).

Thème nº 2 : Transparence

La transparence doit être totale, de sorte que tous les participants (élèves, parents, corps enseignant et administration) puissent aisément comprendre quelles données sont collectées et pourquoi; un consentement éclairé ne peut être donné qu'en connaissance de l'utilisation qui sera faite des données. Les modalités, souvent rédigées en langage technique ou juridique, sont complexes et difficiles à déchiffrer, ce qui constitue un autre obstacle au consentement éclairé. En outre, comme la confidentialité n'est généralement pas expliquée en détail dans les modalités, les utilisateurs restent dans l'ignorance quant à l'utilisation des données qu'ils fournissent : seront-elles employées à des fins autres que celles pour lesquelles elles sont collectées, qui les stocke, et à quel endroit? Les participants ont indiqué que les grandes entreprises (surtout américaines) agrégeaient des données sans consentement. Ils ont aussi fait valoir que les droits d'accès de chaque acteur d'un échange de données (acteur ou sujet, élève ou parent) devraient être limités aux besoins de son rôle, mais que ces droits ne sont pas toujours bien définis.

Thème nº 3 : Uniformité

Les participants ont rapporté une confusion entourant les différentes façons dont les établissements d'enseignement utilisent les outils d'apprentissage numérique comme Teams et Zoom ainsi que les modalités variables qui gouvernent ces outils. Il plane aussi une incertitude quant aux droits de propriété et d'accès relatifs aux données contenues dans les enregistrements, notamment la matière, les réflexions et les informations présentées. On note également une absence de consensus sur la nature du consentement parental, car ce sont les entreprises et non les écoles qui le recueillent. Les participants se sont d'ailleurs demandé si les établissements saisissaient réellement la nature et le pourquoi des activités. Ils ont suggéré de sonder les conseils scolaires pour recueillir l'opinion du corps enseignant et des administrations, ainsi que les élèves pour vérifier l'utilisation qu'ils font des outils d'apprentissage numérique et la compréhension qu'ils en ont. Il y aurait aussi lieu de se renseigner davantage sur les modalités des logiciels et des systèmes.

Thème nº 4 : Technologie

Les participants ont souligné que les écoles exploraient déjà les outils d'apprentissage numérique depuis des années, mais que la COVID-19 avait précipité leur adoption. Les éducateurs ont subi beaucoup de pression pour commencer l'enseignement en ligne et se sont donc rabattus sur les outils les plus simples à utiliser, sans égard à la confidentialité ou la conformité. Il faudra s'assurer que l'emploi actuel de ces outils ne nuise pas au déploiement de nouvelles technologies plus appropriées et sécuritaires.

Q1.2 : Quels règlements, règles ou normes sont en place, à votre connaissance, pour encadrer la surveillance numérique?

Thème nº 5 : Confidentialité

Les participants ont mentionné plusieurs travaux en cours à consulter dans l'élaboration de règlements visant à encadrer divers aspects de la surveillance en ligne. Les voici :

- Identité auto-souveraine; https://docs.igrant.io/ssi/ (système aussi examiné par le gouvernement de la Colombie-Britannique)
- ISO/IEC 29134:2017, *Technologies de l'information – Techniques de sécurité – Lignes directrices pour l'étude d'impacts sur la vie privée*; https://www.iso.org/fr/standard/62289.html
- ISO/IEC WD TS 27560.2, *Privacy technologies – Consent record information structure*; https://www.iso.org/fr/standard/80392.html
- ISO/IEC 24760-1:2019, *Sécurité IT et confidentialité – Cadre pour la gestion de l'identité – Partie 1 : Terminologie et concepts*; https://www.iso.org/fr/standard/77582.html
- Normes publiques; https://standards.iso.org/ittf/PubliclyAvailableStandards/
- Code pour la conception en fonction de l'âge du Royaume-Uni; https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/
- Loi américaine sur le droit à l'éducation et la protection des renseignements personnels des familles (*Family Educational Rights and Privacy Act*)

Le Commissariat à la protection de la vie privée du Canada propose aussi des lignes directrices pour l'obtention d'un consentement valable comprenant une section sur le consentement des enfants (https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/collecte-de-renseignements-personnels/consentement/gl_omc_201805/).

Certains participants ont également indiqué que le Royaume-Uni travaillait à élaborer de nouvelles normes spécialement pour les enfants. Par exemple, au premier trimestre de 2020, le gouvernement a créé des arbres décisionnels visant à mieux comprendre les enfants de différents âges, ainsi que les risques qui les menacent et les façons de les contrer.

Il a toutefois été souligné que les politiques et les règlements futurs devront pouvoir être appliqués pour être efficaces, surtout dans les cas (fréquents) où les données sont envoyées à l'étranger. Le Canada dispose de lois rigoureuses sur le consentement, mais elles ne sont pas toujours applicables sur la scène internationale.

Avenir de la surveillance des enfants et des systèmes d'apprentissage numérique

Dans la deuxième moitié de la discussion, les participants ont été invités à donner leur opinion sur l'avenir souhaité de la surveillance des enfants et des systèmes d'apprentissage numérique.

Q2.1 : Quel est l'avenir idéal de la surveillance en ligne au Canada? (Quelles sont les possibilités idéales, et quels avantages présente la montée en puissance de la surveillance en ligne?)

Thème nº 6 : Collaboration

Les participants estiment que les parents et les éducateurs devraient avoir accès à un environnement adapté et convivial créé par des Canadiens pour les Canadiens. Ils sont d'avis que les données générées et collectées ici doivent rester ici, ce qui implique une dépendance réduite aux entreprises de technologie étrangères. Ils proposent la création d'un répertoire en ligne des fournisseurs de services et de technologies pour renseigner les écoles et les parents. (Les participants ont indiqué qu'aux États-Unis, des enseignants avaient contourné les processus internes de leur école pour intégrer directement des applications à leurs cours.) Une personne a mentionné que des problèmes survenaient parfois lorsque le gouvernement fédéral prévoyait des règles et des règlements auxquels les provinces n'adhéraient pas, et d'autres se sont demandé comment la structure pourrait être modifiée pour corriger la situation.

Thème nº 7 : Sécurité

Il faut mieux définir les rôles et les droits d'accès aux données des entreprises de technologie. La population étant surveillée dans son quotidien, elle doit être habilitée à donner un consentement éclairé, et le gouvernement devrait exercer un plus grand contrôle sur cette surveillance. Il faudrait des mécanismes de gestion de l'identité pour les consentements fournis par des représentants autorisés. La cybersécurité devrait aussi être prise en compte, notamment les efforts des entreprises et des organismes pour renforcer leurs protections. Toutes les règles et tous les règlements devraient reconnaître le droit à l'oubli.

Thème nº 8 : Pratiques exemplaires

Les participants aimeraient voir une meilleure diffusion de pratiques exemplaires sur la formation des parents, des établissements d'enseignement et des élèves. Ils considèrent que les enfants devraient être au cœur de toutes les procédures de gouvernance; idéalement, on maximiserait le contrôle qu'ils ont sur les données transmises aux fournisseurs de services, en permettant par exemple de refuser certaines utilisations, particulièrement celles qui visent à monnayer ou à marchandiser les données. Les systèmes devraient être conçus pour protéger les enfants le mieux possible, selon des principes de confidentialité et de consentement à la collecte des données. En outre, chaque collecte devrait avoir un objectif clair bénéficiant au fournisseur de contenu et à l'utilisateur final. L'un des participants a souligné que BeaconAI travaillait à établir une preuve de confidentialité des données qui offrirait aux utilisateurs une meilleure compréhension de ce qui est collecté et de l'utilisation qui en est faite.

Q2.2 : Quelles sont les répercussions sur le consentement parental de la nouvelle version de la LPRPDE et des normes émergentes de gouvernance des données?

Thème nº 9 : Accès

Il faudrait mieux expliquer aux utilisateurs les options qui s'offrent à eux au moment de donner leur consentement, notamment les conséquences d'un refus potentiel de leur part et les autres possibilités. Par exemple, si un élève (ou son parent) refuse de consentir, perd-il le droit d'assister aux cours? L'enseignant perd-il son droit d'enseigner? Peut-on donner un consentement partiel? Les établissements ont-ils l'obligation d'offrir un autre mode d'enseignement aux personnes qui ne consentent pas?

L'un des participants a dénoncé le danger de ne demander que le consentement parental. En effet, bien que ce soit souvent perçu comme un moyen de protéger les enfants en raison de leur naïveté, force est de reconnaître que certains élèves sont mieux informés sur la technologie que leurs parents ou ont d'autres préférences qu'eux ou que leur école en matière de confidentialité. C'est pourquoi il faudra revoir la hiérarchie des rôles. À l'heure actuelle, les enfants sont au bas de la pyramide, car les parents et les établissements d'enseignement souhaitent les protéger. Or, ils devraient être inclus dans le processus décisionnel et la structure de choix globale. Le recours au consentement parental devrait dépendre de l'âge légal du consentement à la collecte de données en ligne. *Le Règlement général sur la protection des données* (RGPD) de l'Union européenne défend les intérêts des enfants en prévoyant la prise en main du consentement à l'âge de 13 ans. Les plateformes devraient permettre un lien facile et intuitif entre parents et enfants. Il faudrait aussi normaliser la classification du contenu selon l'âge pour qu'il soit plus aisé de comprendre le type de consentement demandé.

Q2.3 : Quels sont les règlements, les règles ou les normes nécessaires pour encadrer la gouvernance des technologies et la surveillance en ligne au Canada?

Thème nº 10 : Sécurité

Les participants ont affirmé la nécessité de réaliser une évaluation des risques associés à la sensibilité des données et aux répercussions des données collectées. Ils ont reconnu que le projet de loi C-11 visait à conformer les règles du Canada au RGPD de l'Union européenne et à la loi sur la protection des renseignements personnels des consommateurs de la Californie, mais ont noté qu'il comportait plusieurs lacunes. Notamment, il rejette la responsabilité d'encadrer les entreprises de technologie sur les autorités de réglementation (ce qui entraîne souvent un comportement évasif de la part des entreprises). Les participants ont aussi fait valoir que la loi de la Californie ne prévoyait pas de justifications normalisées et ne traitait pas directement du consentement parental.

Thème nº 11 : Confidentialité

La confidentialité devrait être prise en considération à toutes les étapes de la définition des modalités, et les preuves de consentement devraient s'intégrer de manière organique au système. Les participants ont suggéré que le Canada établisse ses normes en fonction des lois provinciales ou territoriales les plus strictes actuellement en vigueur. L'un des participants a donné le Québec en exemple pour l'encadrement des modalités.

Annexe E –

Liste des membres du Collectif canadien de normalisation en matière de gouvernance des données (CCNGD)

(Nota : La situation d'emploi et l'organisation d'attache des participants pourraient avoir changé depuis le début du projet.)

Comité directeur du CCNGD

Catégorie/rôle	Prénom	Nom	Titre	Organisme	P/T	Secteur
Milieu universitaire	Adrian Mark	Thorogood	Associé universitaire	Centre de génomique et politiques (CGP), Université McGill	Qc	Santé
Milieu universitaire	Eric M.	Meslin	Ph. D., MACSS, président-directeur général, agrégé supérieur, PHG Foundation, Université de Cambridge	Conseil des académies canadiennes	Ont.	Général
Milieu universitaire **Coprésident du groupe de travail 2**	Michel	Girard	Agrégé supérieur	Centre pour l'innovation dans la gouvernance internationale (CIGI)	Qc	Général
Milieu universitaire	Teresa	Scassa	Professeure, Faculté de droit, section de common law	Université d'Ottawa	Ont.	Consultation
Société civile	Ashley	Casovan	Directrice générale	AI Global	Ont.	Technologies numériques – IA
Société civile	Aubrey	LeBlanc	Directrice générale	Association des officiers en bâtiments de l'Ontario, et présidente du Comité ISO pour la politique en matière de consommation (COPOLCO)	Ont.	Construction
Société civile	Bianca	Wylie	Indépendante	Divers	Ont.	Technologies numériques – Général
Société civile **Coprésidente du groupe de travail 1**	Carole	Piovesan	Associée et cofondatrice	INQ Data Law	Ont.	Technologies numériques – Gestion

Société civile	Carolyn	Watters	Professeure émérite	Université Dalhousie	Ont.	Technologies numériques – Général
Société civile	Chantal	Bernier	Avocate-conseil	Dentons, agrégée supérieure, École supérieure d'affaires publiques et internationales, Université d'Ottawa	Ont.	Technologies numériques – Gestion
Société civile	Jean-Noé	Landry	Directeur général	Nord Ouvert	Qc	Technologies numériques – Général
Société civile	Jonathan	Dewar	Directeur	Centre de gouvernance de l'information des Premières Nations	Ont.	Technologies numériques – Gestion
Gouvernement	André	Loranger	Statisticien en chef adjoint (Études analytiques, méthodologie et infrastructure statistique), dirigeant principal des données	Statistique Canada	Ont.	Services publics – Fédéral
Gouvernement **Coprésident du CCNGD – Secteur public**	Anil	Arora	Statisticien en chef du Canada	Statistique Canada.	Ont.	Services publics – Fédéral
Gouvernement **Coprésident du groupe de travail 3**	Charles	Taillefer	Directeur, Direction de la politique sur la vie privée et la protection des données	Innovation, Sciences et Développement économique Canada (ISDE)	Ont.	Services publics – Fédéral
Gouvernement	Cory	Chobanik	Directeur	Statistique Canada	Ont.	Services publics – Fédéral
Gouvernement **Coprésident du groupe de travail 2**	Eric	Rancourt	Directeur général, Gestion stratégique des données	Statistique Canada	Ont.	Services publics – Fédéral
Gouvernement	France	Pégeot	Première vice-présidente	Agence canadienne d'inspection des aliments (ACIA)	Ont.	Services publics – Fédéral
Gouvernement	Gerard	Peets	Sous-ministre adjoint, Direction générale des politiques et des résultats	Infrastructure Canada	Ont.	Services publics – Fédéral
Gouvernement	Jennifer	Miller	Directrice générale, Gestion stratégique des données	ISDE	Ont.	Services publics – Fédéral
Gouvernement	Jody	Lobb	Directrice exécutive, Planification stratégique intégrée	Secrétariat du Conseil du Trésor	Ont.	Services publics – Fédéral
Gouvernement	Mark	Schaan	Sous-ministre adjoint délégué	ISDE	Ont.	Services publics – Fédéral

Gouvernement	Tracy	Wood	Chef de l'exploitation, Bureau du numérique, Finances, Secrétariat du Conseil du Trésor, Services partagés en technologie de l'information	Gouvernement de l'Î.-P.-É.	Î.-P.-É.	Services publics – Provincial
Industrie	Cam	Vidler	Chef, secteur public	Green Shield Canada (CGC)	Ont.	Santé
Industrie	Dana	O'Born	Directrice, Initiatives stratégiques	Conseil canadien des innovateurs	Ont.	Général
Industrie **Coprésident du groupe de travail 3**	Evgueni	Loukipoudis	Directeur principal, Technologie	Supergrappe des technologies numériques du Canada	C.-B.	Technologies numériques – Général
Industrie	Gord	Beal	Vice-président, Recherche, orientation et soutien	Comptables professionnels agréés (CPA) Canada	Ont.	Services financiers
Industrie **Coprésidente du groupe de travail 4**	Grace	Abuhamad	Chargée de programme de recherche, Trustworthy AI	ServiceNow	Qc	Technologies numériques – IA
Industrie **Coprésidente du groupe de travail 1**	Joni	Brennan	Présidente	Conseil d'identification et d'authentification numériques du Canada (CCIAN)	Ont.	Technologies numériques – Gestion
Industrie **Coprésidente du groupe de travail 4**	Maithili	Mavinkurve	Chef de l'exploitation	Sightline Innovation	Ont.	Technologies numériques – IA
Industrie **Coprésident du CCNGD – Secteur privé**	Philip	Dawson	Responsable des politiques publiques		Qc	Technologies numériques – IA
Normalisation	James (Jim)	MacFie	Agent des normes nationales Président du comité parallèle JTC 1 TC – Technologies de l'information Président canadien du comité parallèle JTC 1/ SC 42 – Intelligence artificielle Vice-président canadien du comité ISO/TC 307 – Technologies des chaînes de blocs et technologies connexes	Microsoft Canada	Ont.	Technologies numériques – Général
Normalisation	Maike	Luiken	Présidente	Institute of Electrical and Electronics Engineers (IEEE) Canada	Ont.	Électronique
Normalisation	Mary	Cianchetti	Présidente, Normes	Groupe Association canadienne de normalisation (CSA)	Ont.	Général

Groupes de travail sur les cas d'usage

Cas d'usage nº 1 – Données sur la santé communautaire	**Eric Sutherlan (président)** Directeur général, stratégie pancanadienne relative aux données sur la santé publique, Agence de la santé publique du Canada **Allie Harris** Vice-présidente et chef des données, Banque Scotia	**Sheriff Abdou** Dirigeant principal des données, Agence de la santé publique du Canada **Eric Rancourt** Directeur général, Gestion stratégique des données, Statistique Canada **Michael Nusbaum** Président, MH Nusbaum & Associates Ltd.
Cas d'usage nº 2 – Identité numérique et systèmes bancaires ouverts	**L'honorable Colin Deacon, sénateur (coprésident)** Sénat du Canada **Joni Brennan (coprésidente)** Présidente, Conseil d'identification et d'authentification numériques du Canada (CCIAN) **Steve Boms** Directeur général, Financial Data and Technology Association (FDATA) **Gene DiMira** Dirigeant principal, Identité, The AML Shop **Franklin Garrigues** Vice-président des canaux numériques, Banque TD **Karim Gillani** Associé directeur, Luge Capital	**Jim Hinton** Fondateur, Own Innovation **Keith Jansa** Directeur général, Conseil stratégique des DPI **Rene McIver** Chef de la sécurité, SecureKey **Kevin Morris** Directeur, Stratégie et programmes, Large Credit Union Council (LCUC) **Mike Penner** Chef de l'exploitation, VoPay **Sylvie Tessier** Membre, Comité d'audit, Bureau du surintendant des institutions financières **Peter Watkins** Directeur des programmes, Institut des services axés sur les citoyens
Cas d'usage nº 3 – Responsabilisation et sécurité des consommateurs : chaînes d'approvisionnement numériques en alimentation	**Brian Kowaluk (président)** Analyste principal, Gestion de l'information et risque, Agence canadienne d'inspection des aliments **Evgueni Loukipoudis** Directeur principal, Technologie, Supergrappe des technologies numériques du Canada **Geoff Isaacs** Responsable de projet, Agence canadienne d'inspection des aliments **Jane Proctor** Vice-présidente, Gestion des politiques et des enjeux, Association canadienne de la distribution de fruits et de légumes **Joe D'Urzo** Directeur principal, Exploitation des données, Les Compagnies Loblaw Limitée	**Maria Paulina Forero, M. Sc.** Ingénieure en bioressources, ingénieure agroalimentaire Spécialiste de secteur, Enjeux multisectoriels, Division de la consultation du secteur, Agriculture et agroalimentaire Canada **Michael Gibbons** Cofondateur et vice-président au développement de produits, Development, Provision Analytics **Nilos Korodimas** Spécialiste de secteur, Enjeux multisectoriels, Direction générale des services à l'industrie et aux marchés, Agriculture et Agroalimentaire Canada **Robyn Edwards** Gestionnaire nationale, Résultats, évaluation et mesure, Agence canadienne d'inspection des aliments **Shubh Singh, MBA** Développement des affaires, Accu-Label

Liste des membres du CCNGD (à l'exclusion du comité directeur)

Organisme	Prénom	Nom	Titre	P/T	Catégorie	Secteur
	Yassen	Atallah	Analyste des politiques		Gouvernement	Santé
	Stefano	Heguy	Étudiant	Ont.	Milieu universitaire	
	Ruben	Sardaryan		Ont.	Industrie	Technologies numériques – Général
Capgemini	Tina	Chakrabarty	Directrice des solutions et des données, Services financiers	Ont.	Industrie	Technologies numériques – Gestion
Institut royal d'architecture du Canada (IRAC)	Louis	Conway	MIRAC, architecte membre de l'Architectural Institute of British Columbia (AIBC)	C.-B.	Société civile	Construction
Alberta Gaming, Liquor and Cannabis	Galina	Rachkova	Architecte des données	Alb.	Gouvernement	Services publics – Provincial
Nation sioux des Nakota d'Alexis	Corrine	St. Dennis	Coordonnatrice de l'accréditation	Alb.	Normalisation	
Alliance of Canadian Building Officials Association	Matthew	Farrell	Vice-président	Ont.	Gouvernement	Construction
Arup Canada Inc.	Justin	Trevan	Associé principal	Ont.	Industrie	
Associated Engineering	Judy	Yu	Gestionnaire des routes	Alb.	Industrie	Consultation
BlackBerry	Takashi	Suzuki	Directeur principal, Normes et développement de la propriété intellectuelle	Ont.	Industrie	Communications
Bloomberg LP	Richard	Beatch	Architecte, sémantique	É.-U.	Industrie	Communications
BlueShore Financial	Janet	Burgess	Vice-présidente, services bancaires de détail/vice-présidente associée, Solutions de veille stratégique	C.-B.	Industrie	Services financiers
BlueShore Financial	Fred	Cook	Dirigeant principal de l'information	C.-B.	Industrie	Services financiers
BlueShore Financial	Rup	Parmar	Vice-présidente, Développement de la technologie des affaires	C.-B.	Industrie	Services financiers
British Columbia Lottery Corporation (BCLC)	Sarah	Marshall	Agente de gouvernance des données	C.-B.	Industrie	
Cambrian Credit Union	Diane	Bilodeau	Vice-présidente principale, Communication avec les membres et veille stratégique	Man.	Industrie	Services financiers
Agence des services frontaliers du Canada	Evelyn	Duberry	Conseillère de programme principale	Ont.	Gouvernement	Services publics – Fédéral

Canada Bridges Consulting; Centre pour l'innovation dans la gouvernance internationale (CIGI)	Marsha	Cadogan	Membre de CIGI Fellow, avocate, consultante propriété intellectuelle et commerce	Ont.	Société civile	Consultation
Inforoute Santé du Canada	Beverly	Knight	Gestionnaire, Normes sur les médicaments	Man.	Société civile	Santé
Canada Vie	Gladiola	Stringa	Directrice, Données d'entreprise	Ont.	Industrie	Services financiers
Administration canadienne de la sûreté du transport aérien (ACSTA)	Gail	McAuliffe	Conseiller principal, Gestion des données	Ont.	Gouvernement	Services publics – Fédéral
Association dentaire canadienne	Dean	Smith	Gestionnaire, Technologies de l'information	Ont.	Industrie	Santé
Association dentaire canadienne	Benoit	Soucy	Directeur des affaires cliniques et scientifiques	Ont.	Industrie	Santé
Agence canadienne d'inspection des aliments	Andrew	Maw	Agent principal des données et du risque	Ont.	Gouvernement	Services publics – Fédéral
Institut canadien d'information sur la santé	Finnie	Flores	Conseillère pédagogique (Normes) et intendante des données de référence	Ont.	Société civile	Santé
Institut canadien d'information sur la santé	Rachel	Hemeon	Chef de programme, Bureau de la gouvernance des données et des normes	Ont.	Société civile	Santé
Institut canadien d'information sur la santé	Eric	Sutherland	Directeur exécutif, Stratégie de gouvernance des données	Ont.	Société civile	Santé
Association canadienne de protection médicale	Om	Patel	Analyste, Relations externes	Ont.	Société civile	Santé
Association canadienne de protection médicale	Daniel	Tardif, M.D.	Directeur, Affaires régionales	Ont.	Société civile	Santé
Société canadienne d'hypothèques et de logement	Joel	Sango	Spécialiste des statistiques d'enquête	Ont.	Gouvernement	Services publics – Fédéral
Conseil de recherche et d'intelligence marketing canadien	John	Tabone	Directeur administratif	Ont.	Industrie	Général
Change Max Consulting	Sherry	Hodge	Responsable internationale, Gestion du changement	C.-B.	Industrie	Consultation
Comptables professionnels agréés (CPA)	Gord	Beal	Vice-président, Recherche, orientation et soutien	Ont.	Industrie	Services financiers
Comptables professionnels agréés (CPA)	Michael	Lionais		Ont.	Industrie	Services financiers
CIBC	Navjit	Singh	Gestionnaire principal, Analyse, lutte contre le blanchiment d'argent	Ont.	Industrie	Services financiers

Institut canadien d'information sur la santé	Paulo	Domingues	Gestionnaire, Opérations d'affaires et d'infrastructure	Ont.	Gouvernement	Santé
Institut canadien d'information sur la santé	Claudiu	Grecu	Architecte des données	Ont.	Gouvernement	Santé
Conseil stratégique des DPI	Keith	Jansa	Directeur général	Ont.	Normalisation	Technologies numériques – Général
Conseil stratégique des DPI	Matthew	MacNeil	Directeur, Normes et technologie	Ont.	Normalisation	Général
Ville de Winnipeg	Chris	Klos	Gestionnaire, Bureau de la gestion des actifs de la Ville, Bureau de la planification en matière d'infrastructure	Man.	Gouvernement	Services publics – Municipal
Cloud Perspectives	Steven	Woodward	Directeur général	Ont.	Industrie	Technologies numériques – Gestion
CloudOps	Ian	Rae	Directeur général	Qc	Industrie	
Cogentas inc.	Luc	Poulin	Directeur général	Qc	Industrie	Technologies numériques – Gestion
Conseil canadien des innovateurs	Dana	O'Born	Directrice, Initiatives stratégiques	Ont.	Industrie	Général
Groupe CSA	Stephen	Michell	Gestionnaire de projet, Normes sur les technologies de l'information et des communications (TIC)	Ont.	Normalisation	Général
Service correctionnel Canada (SCC)	Michael	Elmore	Directeur, Données organisationnelles et gestion de l'information	Ont.	Gouvernement	
Cybersecurity Research Lab	Annegret	Henninger	Chargée de projet	Ont.	Milieu universitaire	Technologies numériques – Général
Denologix	Palle	Johnson	Directeur général, Secteur public	Ont.	Industrie	Technologies numériques – IA
Ministère de la Défense nationale	Julia	Dick	Analyste subalterne des politiques numériques	Ont.	Gouvernement	Services publics – Fédéral
Desjardins	Elisabeth	Diop	Conseillère principale	Qc	Industrie	Services financiers
Conseil d'identification et d'authentification numériques du Canada (CCIAN)	Joni	Brennan	Présidente	Ont.	Industrie	Technologies numériques – Gestion
Environnement et Changement climatique Canada (ECCC)	Elisabeth	Siré	Économiste/analyste en gouvernance des données	Qc	Gouvernement	Services publics – Fédéral
Edge Imaging	Jordan	Moore	Vice-présidente, Marketing et produits	Ont.	Industrie	Services

Edge Imaging	Mike	Watkinson	Dirigeant principal de la technologie et chef de la protection des renseignements personnels	Ont.	Industrie	Services
EllisDon	Rosemarie	Lipman	Dirigeante principale de l'information et vice-présidente principale, Veille stratégique	Ont.	Industrie	Construction
EllisDon	Patrick	To	Gestionnaire, Étude et analyse	Ont.	Industrie	Construction
Environics Analytics	James	Smith	Agent principal de la conformité et de la confidentialité	Ont.	Industrie	Services
Equifax Canada	Ajay	Handa	Directeur des données	Ont.	Industrie	Services financiers
Equifax Canada	Yassir	Jiwan	Chef de l'innovation numérique	Ont.	Industrie	Services financiers
Equifax Canada	Cris	Krnjeta	Analyste de données		Industrie	Services financiers
Excelar Technologies	Colin	Quon	Directeur général	C.-B.	Industrie	Consultation
Financial Data and Technology Association of North America (FDATA)	Steve	Boms	Directeur général	É.-U.	Industrie	Services financiers
FormAssembly	Beenish	Saeed	Représentant, Développement des ventes	Ont.	Industrie	Services
Collège George Brown	Andres	Ponton	Étudiant	Ont.	Milieu universitaire	
Gouvernement de la Colombie-Britannique, ministère de la Santé	Noushin	Nabavi	Économiste	C.-B.	Gouvernement	Services publics – Provincial
Gouvernement de la Saskatchewan Services correctionnels, Services de police et Sécurité publique; Justice et Procureur général	Yashu	Bither	Directeur, Veille stratégique et analyse de données	Sask.	Gouvernement	Services publics – Provincial
Green Shield Canada (CGC)	Adam	Aspinall	Gestionnaire, Étude et analyse des données	Ont.	Société civile	Services
H2O.ai	Bahador	Khaleghi	Scientifique des données des clients	Ont.	Industrie	
Santé Canada	Peggy	Ainslie	Directrice	Ont.	Gouvernement	Santé
Santé Canada	Jenny	Bunning	Analyste des politiques	Ont.	Gouvernement	Santé
Santé Canada	Ben	Diepeveen	Analyste des politiques	Ont.	Gouvernement	Santé
Santé Canada	Jane	Kolbe	Conseillère principale	Ont.	Gouvernement	Santé
Santé Canada	Brett	Taylor	Analyste des politiques	Ont.	Gouvernement	Santé
Holt Renfrew	Kristina	Smith	Agente de protection de la vie privée	Ont.	Industrie	Vente au détail
Banque HSBC Canada	Matthew	Dickinson	Dirigeant principal des données	C.-B.	Industrie	Services financiers
Hydro-Québec	Sanaa	Achaibi	Conseillère, Veille stratégique	Qc	Industrie	Services publics – Provincial

Société indépendante d'exploitation du réseau d'électricité (SIERE)	Lisa	Barnet	Conseillère juridique principale et agente de protection de la vie privée	Ont.	Gouvernement	Services publics – Provincial
Société indépendante d'exploitation du réseau d'électricité (SIERE)	David	Chong Tai	Gestionnaire principal, Compteurs intelligents	Ont.	Gouvernement	Services publics – Provincial
Société indépendante d'exploitation du réseau d'électricité (SIERE)	Sorana	Ionescu	Directrice, Compteurs intelligents	Ont.	Gouvernement	Services publics – Provincial
Société indépendante d'exploitation du réseau d'électricité (SIERE)	Erin	Williams	Superviseure, gouvernance de l'information	Ont.	Gouvernement	Services publics – Provincial
Conseil des technologies de l'information et des communications	Rob	Davidson	Directeur, Analyse des données	Ont.	Industrie	Communications
Division de l'information, de la protection de la vie privée et des Archives publiques	John	Roberts	Directeur général de la protection de la vie privée et archiviste de l'Ontario	Ont.	Gouvernement	Services publics – Provincial
Infoset	Varinder	Sembhi	Associé directeur	Ont.	Industrie	
Infrastructure Canada	Lucy	Opsitnik	Gestionnaire de données	Ont.	Gouvernement	Services publics – Fédéral
Interac	Aruna	Dorai	Directrice	Ont.	Industrie	Services financiers
ISDE	Dashiell	Dronyk	Conseiller en politiques, Direction de la politique sur la vie privée et la protection des données	Ont.	Gouvernement	Services publics – Fédéral
ISDE	Jacqueline	Jones	Conseillère en politiques, Direction de la politique sur la vie privée et la protection des données	Ont.	Gouvernement	Services publics – Fédéral
KPMG	Najib	Bounouane	Gestionnaire, Gouvernance de l'information et des données	Qc	Industrie	Services
KPMG	Catherine	Nadeau	Gestionnaire principale, Gouvernance de l'information	Qc	Industrie	Services
Programme du travail – Emploi et Développement social Canada (EDSC)	Jason	Maurice	Analyste principal des politiques	Qc	Gouvernement	Services publics – Fédéral
Programme du travail – Emploi et Développement social Canada (EDSC)	Abhinav	Rao	Agent d'analyse statistique des données	Qc	Gouvernement	Services publics – Fédéral
Programme du travail – Emploi et Développement social Canada (EDSC)	David	Santos	Analyste	Qc	Gouvernement	Services publics – Fédéral

Large Credit Union Coalition	Kevin	Morris	Directeur, Stratégie et programmes	Ont.	Industrie	Services financiers
LifeSciences BC	Wendy	Hurlburt	Présidente et directrice générale	C.-B.	Industrie	Général
Les Compagnies Loblaw Limitée	Alessandra	Bresani	Directrice, Protection des renseignements personnels	Ont.	Industrie	Vente au détail
Les Compagnies Loblaw Limitée	John	Nicodemo	Vice-président, Ingénierie des données	Ont.	Industrie	Vente au détail
MH Nusbaum & Associates Ltd.	Michael	Nusbaum	Président	C.-B.	Industrie	Santé
Société d'assurance publique du Manitoba	Daniel	Faingold	Gestionnaire, Analyse des activités	Man.	Gouvernement	Services financiers
Société d'assurance publique du Manitoba	Lawrence	Lazarko	Directeur, Information et technologie	Man.	Gouvernement	Services financiers
Société d'assurance publique du Manitoba	Divya	Polavaram	Gestionnaire	Man.	Gouvernement	Services financiers
Mapador	Sam	Malek	Directeur principal de la technologie	Ont.	Industrie	Technologies numériques – Général
Mature-ITSM inc.	Andre	Boutin	Consultant, Gouvernance numérique	Qc	Industrie	Technologies numériques – Gestion
Université McMaster / Réseau canadien des centres de données de recherche	Michael	Veall	Professeur en économie et chercheur principal	Ont.	Milieu universitaire	Technologies numériques – Général
Université McMaster / Institut Vecteur	Ranil	Sonnadara	Conseiller spécial au vice-recteur (Recherche) / professeur agrégé	Ont.	Milieu universitaire	
Minerva Intelligence Inc.	Jake	McGregor	Chef de l'exploitation	C.-B.	Industrie	Technologies numériques – IA
S. O.	Vasiliki (Vass)	Bednar	Simple citoyen	Ont.	Société civile	Technologies numériques – Général
S. O.	Jeremy	Depow	Intervenant indépendant	Ont.	Industrie	Technologies numériques – Gestion
NetGovern	Pierre	Chamberland	Directeur général	Qc	Industrie	Technologies numériques – Gestion
Newcomp Analytics / Université de Toronto	Mareena	Mallory	Scientifique des données et chargée de cours	Ont.	Milieu universitaire	Technologies numériques – Général
Newport Thomson	Derek	Lackey	Directeur général	Ont.	Industrie	Technologies numériques – Gestion
Northern Credit Union	Chris	Armenti	Vice-président associé – Solutions d'affaires	Ont.	Industrie	Services financiers
Organisme d'autoréglementation du courtage immobilier du Québec (OACIQ)	Dominique	Derome	Vice-présidente, Finances, TI et processus d'affaires	Qc	Gouvernement	

Organisme d'autoréglementation du courtage immobilier du Québec (OACIQ)	Caroline	Simard	Vice-présidente, Gouvernance	Qc	Gouvernement	
Association des officiers en bâtiments de l'Ontario/Cité de Windsor, Services du bâtiment	Leslie	Wright	Spécialiste en transformation numérique	Ont.	Gouvernement	Services publics – Municipal
Octane Biotech Inc.	Chaitanya	Baliga	Chef, Qualité	Ont.	Industrie	Santé
Commissariat à la protection de la vie privée du Canada	Thibault	Lacroix	Gestionnaire, Programmes et services de gestion de l'information	Ont.	Gouvernement	Services publics – Fédéral
Société des loteries et des jeux de l'Ontario	Allie	Harris	Directrice, Gouvernance de l'information organisationnelle	Ont.	Gouvernement	Services publics – Provincial
Institut universitaire de technologie de l'Ontario	Andrea	Slane	Professeure agrégée	Ont.	Milieu universitaire	Général
Open City Network	Andy	Best	Directeur général	Ont.	Société civile	Technologies numériques – IA
Nord Ouvert – Laboratoire de recherche appliquée	Steven	Coutts	Analyste de recherche	Qc	Société civile	Technologies numériques – Général
Opris & Associates Inc.	Candid	Opris	Directeur et associé	Ont.	Industrie	
Own Innovation	Jim	Hinton	Avocat, agent de brevets et de marques de commerce	Ont.	Industrie	Consultation
Paiements Canada	Craig	Borysowich	Directeur, Intégration et normes	Ont.	Industrie	Services financiers
Paiements Canada	Judy	Li	Gestionnaire, Information et analyse de données	Ont.	Industrie	Services financiers
PBC & Associates	Paul	Cotton	Fondateur et propriétaire	C.-B.	Industrie	Technologies numériques – Général
Ministère des Finances de l'Î.-P.-É., Services de TI partagés	Nan	Court	Gestionnaire, Services de données	Î.-P.-É.	Gouvernement	Services publics – Provincial
Ministère des Finances de l'Î.-P.-É., Services de TI partagés	Roman	Embleton	Architecte des données	Î.-P.-É.	Gouvernement	Services publics – Provincial
Agence de la santé publique du Canada (ASPC)	Rita	Finley	Analyste principale des politiques, Bureau du conseiller scientifique principal	Ont.	Gouvernement	Services publics – Fédéral
Plaid	John	Pitts	Chef, Politiques	É.-U.	Industrie	Services financiers
Plaid	Ben	White	Recherche et développement, Politiques	É.-U.	Industrie	Services financiers

Portag3 Ventures	Ben	Harrison	Associé, Chef des partenariats et des politiques	Ont.	Industrie	Services financiers
Corporation financière Power	Pierre	Piché	Vice-président	Qc	Industrie	Services financiers
Professional Petroleum Data Management Association	Trudy	Curtis	Directrice générale	Alb.	Industrie	Énergie
Protein Industries Canada	Ken	Sackley	Dirigeant principal de l'Information – Chef des données	Ont.	Industrie	Santé
PSD Research, Consulting Software	Matthew	Dawe	Vice-président	Ont.	Industrie	Consultation
PSD Research Consulting Software	Tyler	Sutton	Directeur général, Recherche et Marketing	Ont.	Industrie	Consultation
Agence de la santé publique du Canada (ASPC)	Susan	Ternan	Centre des données, des partenariats et de l'innovation	Ont.	Gouvernement	Santé
Public Sector Digest	Chris	Vanderheyden	Consultant principal, Gestion des actifs	Ont.	Industrie	Consultation
PwC	Cristina	Onosé	Leader, Défense de la vie privée et conseils d'experts	Ont.	Industrie	Services
Quantum-Safe Canada	Bill	Munson	Directeur, Recherche et analyse des politiques	Ont.	Milieu universitaire	Technologies numériques – Gestion
Questrade	Ernani	Cecon	Directeur, Architecture d'entreprise	Ont.	Industrie	Services financiers
RBC	Lisa Marie	Daulby	Directrice, Gouvernance des politiques sur les données organisationnelles	Ont.	Industrie	Services financiers
RBC	Don	Dela Paz	Vice-président, Risque en gestion de l'information, Bureau principal des données	Ont.	Industrie	Services financiers
RBC	Ajinkya	Kulkarni	Directeur principal, Science des données	Ont.	Industrie	Services financiers
RBC	Catherine	Stephen	Conseillère principale	Ont.	Industrie	Services financiers
Régie de l'assurance maladie du Québec	Denis	Côté	Conseiller en architecture d'entreprise – Volet information	Qc	Gouvernement	Services publics – Municipal
Données de recherche Canada	Mark	Leggott	Directeur exécutif	Ont.	Société civile	Services
Conseil canadien du commerce de détail	Kate	Skipton	Analyste principale de politiques	Ont.	Industrie	Vente au détail
Risk Management Association Toronto / CGG Consulting	Stella	Cabrera	Présidente fondatrice	Ont.	Industrie	Services financiers
Comité parallèle du CCN ISO/PC 317	Graham Rae	Dulmage	Président	Ont.	Normalisation	Consultation
Secrétariat du Conseil du trésor (SCT)	Marc	Vézina	Directeur de l'architecture d'entreprise gouvernementale	Qc	Gouvernement	Général

SecureKey Technologies	Rene	McIver	Chef de la sécurité et de la protection des renseignements personnels	Ont.	Industrie	Technologies numériques – Gestion
SecureKey Technologies	Eric	Swedersky	Vice-président directeur, Secteur public et prestation de service	Ont.	Industrie	Technologies numériques – Gestion
Service Nouveau-Brunswick	Erin	Hardy	Chef de la protection de la vie privée	N.-B.	Gouvernement	Services publics – Provincial
Shaw Communications	Sangeetha	Varghese	Gestionnaire, Gouvernance des données et qualité	Alb.	Industrie	Communications
SiMPACT	Stephanie	Robertson	Fondatrice et directrice générale	Ont.	Industrie	Services financiers
Slack Consulting	Ellen	Brown	Analyste, Veille stratégique	Ont.	Industrie	Consultation
Smart City	Steve	Czajka	Gestionnaire	Ont.	Gouvernement	Technologies numériques – IA
Smart Species	Mark	Lizar	Directeur général	Ont.	Industrie	Consultation
Conseil de recherches en sciences humaines	Ariadne	Legendre	Gestionnaire, Analyse de l'organisation et des affaires	Ont.	Gouvernement	Général
Sparkgeo	James	Banting	Développeur	C.-B.	Industrie	Consultation
Statistique Canada	Tom	Dufour	Directeur général, Gestion stratégique des données	Ont.	Gouvernement	Services publics – Fédéral
Statistique Canada	Sevgui	Erman	Directrice, Division de la science des données	Ont.	Gouvernement	Services publics – Fédéral
Statistique Canada	Julie	Trépanier	Directrice, Division de l'infrastructure d'intégration de données	Ont.	Gouvernement	Services publics – Fédéral
Sun Life Canada	Paul	Mendes	Directeur principal, Gouvernance des données	Ont.	Industrie	Services financiers
Secrétariat du Conseil du Trésor du Canada, Bureau du dirigeant principal de l'information	Omar	Bitar	Conseiller (données organisationnelles et IA)	Ont.	Gouvernement	Services publics – Fédéral
Groupe Banque TD	Jennifer	Gibbs	Dirigeante principale des données	Ont.	Industrie	Services financiers
TD Assurance	Sophiya	Varghese	Gestionnaire principale, Gouvernance des données, données et vision	Qc	Industrie	Services financiers
Tehama	Karen	Chase	Directrice, Programmes sectoriels et gouvernementaux	Ont.	Industrie	Technologies numériques – Général
TELUS	Jesslyn	Dymond	Spécialiste, IA responsable	Ont.	Industrie	Communications
TELUS	Elena	Novas	Directrice, Renseignements personnels et innovation	Ont.	Industrie	Communications
TELUS Communications	Carine	Botturi	Directrice, Gestion du risque, Bureau du chef des données et des relations de confiance	Qc	Industrie	Communications

Centre de recherche informatique de Montréal	Fehmi	Jaafar	Chercheur en cybersécurité	Qc	Milieu universitaire	Technologies numériques – Général
Thomson Reuters	Cormac	Brady	Dirigeant principal de la technologie, Plateformes et contenu	É.-U.	Industrie	Communications
ToP KaTS	Michael	Lamoureux	Président	N.-É.	Industrie	Consultation
Chambre de commerce de la région de Toronto	Thomas	Goldsmith	Directeur des politiques, Innovation et technologie	Ont.	Industrie	Général
TransUnion of Canada Inc.	Heather	Burke	Gestionnaire principale, Gestion des données	Ont.	Industrie	
TransUnion of Canada Inc.	Johanna	FitzPatrick	Conseillère juridique et agente de protection de la vie privée	Ont.	Industrie	
TransUnion of Canada Inc.	Iain	Page	Conseiller, Stratégie de données	Ont.	Industrie	
TransUnion of Canada Inc.	Alison	Paisley	Gestionnaire, Acquisition de données	Ont.	Industrie	
Transports Canada	Dominic	Canuel	Gestionnaire, Gestion des données	Ont.	Gouvernement	Services publics – Fédéral
Secrétariat du Conseil du Trésor	Jason	Blackwell	Stratège principal, Bureau du dirigeant principal de l'information	Ont.	Gouvernement	
Secrétariat du Conseil du Trésor	Michael	Goit	Directeur, Identité numérique	Ont.	Gouvernement	Services publics – Fédéral
Secrétariat du Conseil du Trésor	Dawn	Hall	Conseillère	Ont.	Gouvernement	
TrustBIX Inc.	Tom	Ogaranko	Dirigeant principal de l'innovation	Alb.	Industrie	Technologies numériques – Général
Normes ULC	Gillian	Wintonic	Chargée de projet	Ont.	Normalisation	Général
Université de Guelph	Rozita	Dara	Professeure adjointe	Ont.	Milieu universitaire	Technologies numériques – Gestion
Université de Victoria	Yvonne	Coady	Professeure	C.-B.	Milieu universitaire	Technologies numériques – Général
UrtheCast	William	Parkinson	Gestionnaire, Produits techniques	C.-B.	Industrie	Technologies numériques – Général
Valencial IIP Advisors Ltd.	Michael	Power	Directeur général, Confidentialité	Ont.	Industrie	Technologies numériques – Gestion
Institut Vecteur	Andrea	Smith	Directrice des partenariats sur les données de santé	Ont.	Milieu universitaire	Technologies numériques – IA
VersaFile Inc.	Darren	Peloso	Directeur de la technologie	C.-B.	Industrie	Technologies numériques – Général
VoPay International Inc.	Mike	Penner	Chef de l'exploitation	C.-B.	Industrie	Services financiers
WMC	Mike	Hughes	Affilié	Alb.	Industrie	Consultation
WSP Canada	Lucy	Casacia	Vice-présidente, Solutions interconnectées	Ont.	Industrie	Technologies numériques – Général

Secrétariat du CCNGD

Rôle	Prénom	Nom	Titre	Organisme
Secrétaire du CCNGD	Anneke	Olvera	Directrice, Programmes et opérations, Stratégie et engagement des intervenants	Conseil canadien des normes
Secrétariat du CCNGD	Brendan	McManus	Gestionnaire, Innovation	Conseil canadien des normes
Secrétariat du CCNGD	Alexandra	Wells	Chargée de projets, Innovation	Conseil canadien des normes
Secrétaire du groupe de travail 1	Alex	Héroux	Spécialiste de secteurs, Innovation	Conseil canadien des normes
Secrétaire du groupe de travail 2	Martin-J.	Beaulieu	Chef, Centre de collaboration internationale et d'innovation en méthodologie	Statistique Canada
Secrétaire du groupe de travail 3	Andrew	Kostruba	Chargé de projet	Groupe CSA
Secrétaire du groupe de travail 3	Edwin	Ndatuje	Spécialiste de secteurs, Innovation	Conseil canadien des normes
Secrétaire du groupe de travail 4 et du cas d'usage n° 1 – Données sur la santé communautaire	Marta	Janczarski	Spécialiste de secteurs, Innovation	Conseil canadien des normes
Secrétaire du cas d'usage n° 2 – Identité numérique et systèmes bancaires ouverts	Dominik	Brejta	Spécialiste de secteurs, Innovation	Conseil canadien des normes
Cas d'usage n° 3 – Responsabilisation et sécurité des consommateurs : chaînes d'approvisionnement numériques en alimentation	Hana	Qowrah	Spécialiste de secteurs, Innovation	Conseil canadien des normes
Responsable de la recherche et de la rédaction du compendium	Diane	Liao	Chargée de programme, Recherche	Conseil canadien des normes
Recherche et rédaction du compendium	Inbal	Marcovitch	Conseillère spéciale, Bureau de la directrice générale	Conseil canadien des normes

Annexe F –

Liste des acronymes et abréviations

Acronyme	Nom
A2F	authentification à deux facteurs
ANSI	American National Standards Institute
API	interface de programmation d'application
ASCE	American Society of Civil Engineers
ASTM	American Society for Testing and Materials
AWWA	American Water Works Association
BSi	British Standards Institution
C4DC	Contracts for Data Collaboration
CCIAN	Conseil d'identification et d'authentification numériques du Canada
CCN	Conseil canadien des normes
CCNGD	Collectif canadien de normalisation en matière de gouvernance des données
CCPT	Comité consultatif des provinces et territoires
CEN	Comité Européen de Normalisation
CENELEC	Comité Européen de Normalisation Électrotechnique
CGIPN	Centre de gouvernance de l'information des Premières Nations
CHIMA	Association canadienne interprofessionnelle du dossier de santé
CIE	Commission Internationale de l'Éclairage
CLSI	Clinical and Laboratory Standards Institute
CSA	Association canadienne de normalisation
CSDPI	Conseil stratégique des DPI
DAMA	Data Management Association
DCAM	modèle d'évaluation des capacités de gestion des données
DIN	German Institute for Standardization
DME	dossier médical électronique

DS	Danish Standards
EDMC	Enterprise Data Management Council
ETSI	European Telecommunications Standards Institute
GOST	Gosstandart (organisme de normalisation russe)
HIMSS	Healthcare Information and Management Systems Society
IA	intelligence artificielle
IAPP	Association internationale des professionnels de la protection de la vie privée
ICIS	Institut canadien d'information sur la santé
IdO	Internet des objets
IEC	Commission électrotechnique internationale
IEEE	Institute of Electrical and Electronics Engineers
ISDE	Innovation, Sciences et Développement économique Canada
ISO	Organisation internationale de normalisation
JTC 1	Comité technique mixte 1
LOINC	Logical Observation Identifiers Names and Codes
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
MDR	registre de métadonnées
MFI	Cadre du métamodèle pour l'interopérabilité
NCBI	National Center for Biotechnology Information
NEMA	National Electrical Manufacturers Association
NFPA	National Fire Protection Association
NIST	National Institute of Standards and Technology
OEN	organisme d'élaboration de normes
ONGC	Office des normes générales du Canada
RGPD	Règlement général sur la protection des données
SNZ	Standards New Zealand
STI	systèmes de traitement de l'information
TI	Technologies de l'information
UIT-R	Union internationale des télécommunications – Secteur des Radiocommunications – Recommandations
UIT-T	Union internationale des télécommunications – Secteur de la normalisation des télécommunications
ULC	Laboratoires des assureurs du Canada
W3C	Consortium World Wide Web

Annexe G –

Paysage normatif du Collectif canadien de normalisation en matière de gouvernance des données (CCNGD) : méthode d'élaboration

La feuille de route s'inspire du cycle de vie de la gouvernance des données. Complexe et mouvant, celui-ci évolue et s'adapte constamment, et fait intervenir beaucoup de parties. Les activités d'élaboration de la feuille de route ont été regroupées sous quatre grands thèmes : 1) Fondements de la gouvernance des données, 2) Collecte, organisation et classement, 3) Accès, diffusion et conservation, 4) Analyse, solutions et commercialisation. Pour chacun de ces thèmes, une liste de sujets généraux a été dressée en lien avec les normes et programmes de conformité sur la gouvernance des données.

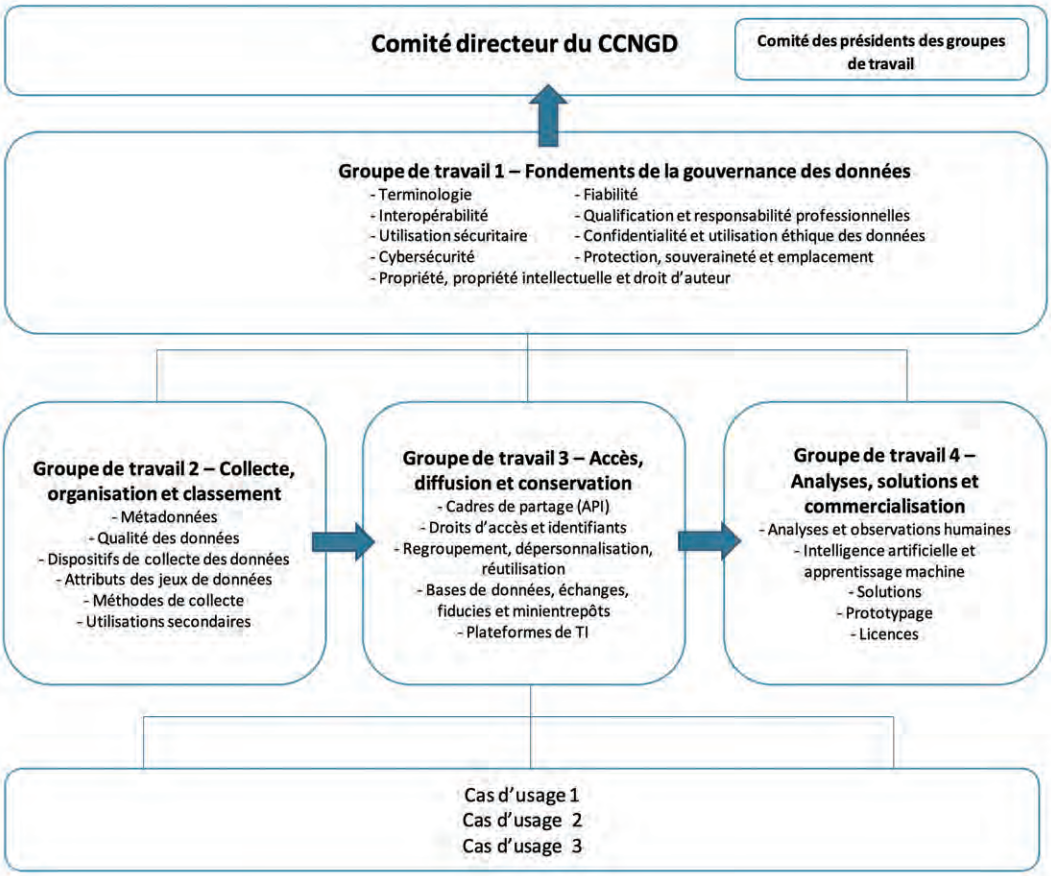
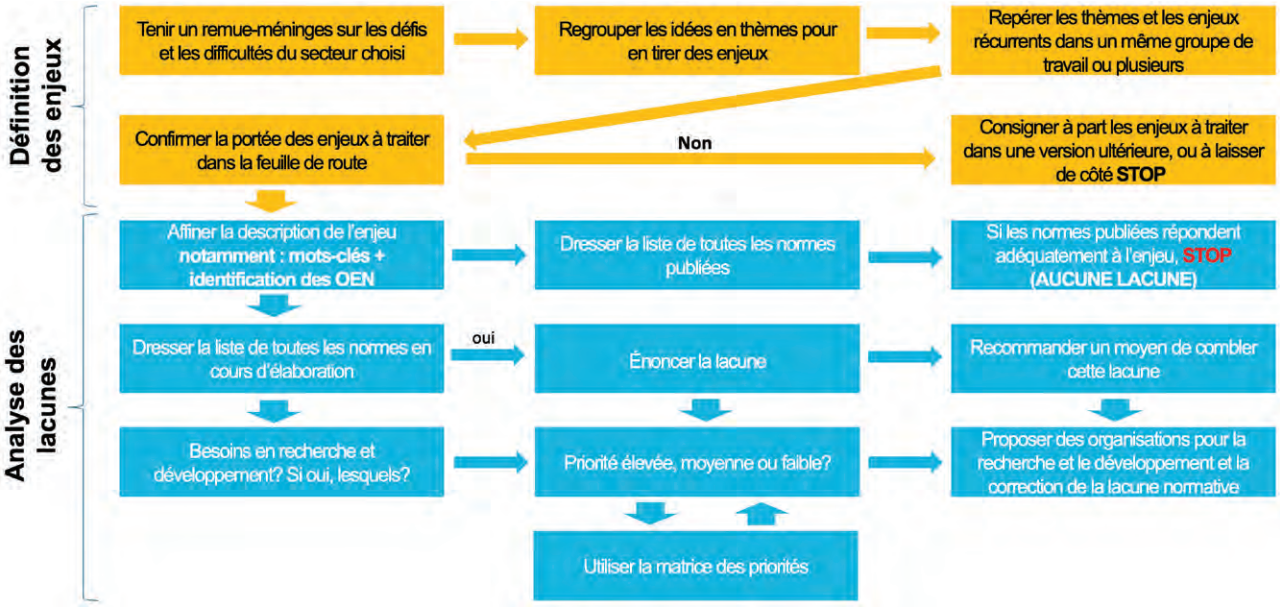


Diagramme 1 : Structure du CCNGD et de la feuille de route

Après avoir tenu, en janvier 2020, une rencontre de lancement de la phase 1, où ils ont soumis à un vote et confirmé les secteurs prioritaires pour la première version de la feuille de route (voir diagramme 2), les groupes de travail ont tenu des réunions en ligne toutes les deux semaines pour décrire les principaux enjeux et en définir la portée, répertorier les normes existantes, analyser les lacunes et rédiger la feuille de route.



L'évaluation de la pertinence des normes pour le CCNGD était une tâche colossale, étant donné l'ampleur du sujet et l'importance des défis posés par les nouvelles technologies dans l'ensemble de la chaîne d'approvisionnement des données et du cycle de vie de la gouvernance des données. Par conséquent, le CCNGD a adopté une méthode de recherche participative afin de permettre à tous les membres des groupes de travail d'apporter leur expertise et leur perspective au processus de production des connaissances, c'est-à-dire à l'élaboration de la feuille de route pour la normalisation[90].

Plus précisément, chaque groupe de travail a suivi les étapes suivantes pour dessiner le paysage normatif actuel dans le domaine qui lui avait été attribué.

90 Bergold, J. et S. Thomas (2012). « Participatory research methods: A methodological approach in motion ». *Historical Social Research/Historische Sozialforschung*, vol. 37, n° 4, p. 191-222.

RÉPERTORIER LES GRANDS THÈMES ET DÉFIS

Les membres de chaque groupe de travail ont dressé ensemble une liste des principaux thèmes, défis, lacunes et possibilités relevant du domaine qui leur avait été attribué. Pour ce faire, ils se sont posé les questions suivantes :

- Quels sont les besoins sociaux, technologiques, économiques, environnementaux, politiques ou relatifs aux valeurs?
- Quels grands changements survenus dans ces secteurs posent des difficultés particulières?
- Y a-t-il des occasions à saisir, mais qui nécessiteraient des solutions de normalisation?

Les groupes de travail ont analysé les résultats de chaque séance de remue-méninges pour les regrouper en thèmes et en tirer des enjeux globaux. Ils ont également défini des sous-sections pour chaque enjeu, et repéré les thèmes et enjeux récurrents dans les différents groupes de travail. Au total, 821 notes ont été consignées, puis regroupées en 53 enjeux.

PRIORISER LES PRINCIPAUX ENJEUX

Une fois les enjeux globaux définis, les groupes de travail les ont passés en revue et leur ont attribué un degré de priorité (par vote). Ainsi, pour chaque enjeu, ils ont répondu aux questions suivantes :

- Quelle est la proposition de valeur?
- Êtes-vous d'accord avec la portée proposée pour l'enjeu?
    - Si oui : Vote sur le degré de priorité (élevé, moyen ou faible); Vote sur le groupe de travail qui devrait être responsable de cet enjeu.
    - Si non : Analyse de l'enjeu pour arriver à un consensus, puis vote.

Parmi les 53 enjeux d'abord proposés, 10 ont été fusionnés parce que leurs portées se recoupaient, 14 ont été mis de côté à cause de leur faible priorité ou de leur manque de clarté, et 6 se sont ajoutés. La liste finale comportait donc 35 enjeux à intégrer à la feuille de route pour la normalisation.

ÉNONCER LES ENJEUX ET LES MOTS-CLÉS

Chaque groupe de travail a analysé les enjeux qui lui ont été confiés pour en définir la portée et en rédiger une description. Il s'agissait notamment de :

- décrire l'enjeu et son importance d'un point de vue commercial, civil ou de sécurité publique;
- proposer une liste de mots-clés à utiliser pour repérer les normes associées à l'enjeu ou aux défis connexes;
- repérer les organismes d'élaboration de normes (OEN) pertinents en fonction de l'enjeu et de la portée de la feuille de route.

Le résultat : plus de 500 mots clés pour les 35 enjeux.

CHERCHER LES NORMES PUBLIÉES

À partir de la liste des mots-clés, les chercheurs du CCN ont fait une recherche pour trouver les normes pertinentes sur IHS, une base de données externe qui répertorie des codes et des normes de plus de 200 OEN du monde entier[91]. Ils se sont donné des critères pour repérer les normes les plus intéressantes pour le CCNGD, notamment :

- ne retenir que la dernière version (en vigueur) d'une norme;
- ne retenir que les normes rédigées en anglais et en français;
- éliminer les normes repérées en double avec des mots-clés différents pour le même enjeu, mais les conserver si elles concernent des enjeux différents (parce qu'elles répondent à des besoins différents);
- éliminer les multiples adoptions d'une même norme pour ne conserver que la norme internationale d'origine.

Au total, environ 12 000 normes ont été repérées pour les 35 enjeux, une fois les doublons éliminés[92].

VALIDER ET TRIER LES NORMES

Il a ensuite fallu valider et trier les normes repérées dans la base de données IHS pour s'assurer de n'oublier aucune norme pertinente et éliminer les autres. Les groupes de travail ont passé en revue la liste de normes et appliqué le code de couleur suivant :

Niveau	Description
I	La norme, selon son titre et sa référence, correspond non seulement aux mots-clés, mais également à la description de l'enjeu; elle semble pouvoir répondre aux préoccupations exprimées.
II	La norme, selon son titre et sa référence, correspond partiellement soit aux mots-clés soit à la description de l'enjeu; elle pourrait répondre partiellement à la préoccupation exprimée ou constituer une référence utile pour la création d'une norme y répondant.
III	La norme, selon son titre et sa référence, n'aurait qu'une utilité très limitée, par exemple dans un secteur précis ou selon une approche nichée.
IV	La norme, selon son titre et sa référence, n'a pas de rapport avec l'enjeu ou les mots-clés.

Une fois cet examen terminé, les résultats ont été envoyés aux OEN concernés, qui les ont commentés et validés. On a aussi demandé aux OEN de dresser une liste de normes en cours de rédaction qui pourraient correspondre aux 35 enjeux définis.

91 IHS Markit. Engineering Workbench: Standards, Codes & Specs. https://ihsmarkit.com/products/standards-codes-specs.html
92 Au départ, la recherche des quelque 500 mots-clés a généré environ 25 000 normes, dont plus de la moitié étaient des doublons à supprimer.

On a ensuite demandé aux groupes de travail d'analyser les lacunes, c'est-à-dire de repérer pour chaque enjeu les normes, spécifications et programmes de conformité nécessaires, mais encore inexistants. Était considérée comme une « lacune » l'absence de norme ou de spécification publiée couvrant l'enjeu en question. Après avoir repéré et décrit une lacune, le groupe de travail formulait des recommandations sur la nécessité de mener des activités de recherche et développement avant la normalisation, sur la façon de combler la lacune, sur son degré de priorité et sur un ou plusieurs organismes (ex. : OEN ou organisme de recherche) qui pourraient s'occuper des activités de recherche et développement ou de la normalisation compte tenu de son domaine d'activité (sans ordre particulier).

Chaque lacune a été évaluée selon les critères qui suivent classée selon son degré de priorité : élevé (à combler en moins de deux ans), moyen (à combler en deux à cinq ans) ou faible (à combler en plus de cinq ans).

Diagramme 3 : Critères de priorité

Critères C-A-P-E (pour établir le niveau de priorité)	Cotes
Caractère critique (répercussions sur la sécurité ou la qualité) – Quelle est l'importance du projet? Est-il urgent de disposer d'une norme ou de lignes directrices? Quelles seraient les conséquences si le projet n'était pas lancé, ou pas mené à bien? Plus la cote est élevée, plus le projet est critique.	3 – critique; 2 – assez critique; 1 – pas critique
Avancement (temps nécessaire) – Est-il logique de lancer ce projet maintenant, compte tenu des autres projets? Le projet est-il nouveau ou déjà en cours? Plus la cote est élevée, plus il est probable que le projet se termine bientôt.	3 – presque terminé; 2 – en cours; 1 – nouveau
Portée (ressources à investir) – Le projet demande-t-il beaucoup de temps, d'énergie et d'argent? Peut-il être réalisé avec les renseignements, les outils et les ressources actuellement disponibles? Faudra-t-il mener des recherches avant la normalisation? Plus la cote est élevée, moins le projet nécessitera de nouvelles ressources.	3 – peu de nouvelles ressources; 2 – un certain nombre de nouvelles ressources; 1 – beaucoup de nouvelles ressources
Effet (rendement) – Une fois terminé, quel effet aura le projet sur la gouvernance des données? Plus la cote est élevée, plus les gains pour le secteur sont importants.	3 – rendement élevé; 2 – rendement moyen; 1 – rendement faible

Signification de la cote totale : Priorité élevée (cote de 10 à 12); priorité moyenne (cote de 7 à 9); priorité faible (cote de 4 à 6).

À la feuille de route s'ajoute le *Paysage normatif du CCNGD*, un tableau des normes liées (directement ou indirectement) aux enjeux décrits dans la feuille de route. On le trouvera à l'annexe I.

Annexe H –

Brève description des organismes d'élaboration de normes (OEN) et autres entités en gouvernance des données

Organisme	Description
Alliance FIDO	L'Alliance FIDO est une association sectorielle ouverte axée sur les normes d'authentification qui cherche à réduire la dépendance aux mots de passe. Elle encourage le développement, l'utilisation et le respect des normes pour l'authentification et l'attestation des dispositifs. Elle compte parmi ses membres plusieurs grandes multinationales, dont Amazon, American Express, Apple, Bank of America, Facebook, Google, Intel, Microsoft, Qualcomm, Samsung, Visa et Wells Fargo.
American Society of Civil Engineers (ASCE)	Les normes de l'ASCE établissent des lignes directrices techniques sur la sécurité, la fiabilité, la productivité et l'efficacité en génie civil. L'ASCE en a publié plus de 60.
American Water Works Association (AWWA)	L'AWWA publie des normes consensuelles sur les équipements et matériaux utilisés dans le traitement et la distribution d'eau potable, pour assurer la construction, l'entretien et l'exploitation de systèmes de traitement et de distribution d'eau supérieurs.
ASTM International (ASTM)	ASTM International (autrefois l'American Society for Testing and Materials) est un leader de l'élaboration et de la production de normes volontaires et consensuelles. Comptant plus de 140 pays membres, elle a publié plus de 12 800 normes dans le monde.
British Standards Institution (BSI)	BSI est l'organisme de normalisation national du Royaume-Uni. Cet organisme de distribution sans but lucratif offre des services partout dans le monde dans plusieurs domaines connexes : normalisation, évaluation des systèmes, certification de produits, formation et conseil. Il crée des normes techniques sur toute une gamme de produits et de services, et offre des services de certification et autres services normatifs aux entreprises.
Centre de gouvernance de l'information des Premières Nations (CGIPN)	Le Centre de gouvernance de l'information des Premières Nations est un organisme sans but lucratif indépendant, apolitique et technique régi par un mandat spécial des Chefs de l'Assemblée des Premières Nations (résolution n° 48, décembre 2009). Le CGIPN a pour vocation de produire de l'information de qualité contribuant à la santé et au bien-être des membres des Premières Nations au Canada. En collaboration avec ses partenaires régionaux, il mène des initiatives uniques de collecte de données pour aider les gouvernements des Premières Nations à brosser un tableau culturellement pertinent de leurs communautés. Le CGIPN appuie les communautés des Premières Nations en contribuant directement au renforcement des capacités en matière de données et de statistiques à l'échelle nationale, régionale et communautaire, notamment en leur fournissant des données crédibles et pertinentes sur les Premières Nations. En plus de mener des sondages, le CGIPN se charge de tout un éventail de travaux : supervision de la collecte de données dans les réserves des Premières Nations et les collectivités du Nord, recherches, traduction et diffusion des connaissances, formation et promotion des principes de PCAP® des Premières Nations. Il faut souligner que le CGIPN et ses partenaires régionaux suivent des protocoles, politiques et procédures basés sur un cadre culturel holistique. En résumé, le CGIPN est un outil qui permet aux Premières Nations détentrices de droits, dans le cadre de leur gouvernance, d'affirmer leur souveraineté sur leurs données et leurs renseignements. Les principes de PCAP® des Premières Nations établissent les modes de collecte, de protection, d'utilisation et de communications des données de celles-ci. Ils constituent un outil qui renforce la gouvernance des données et l'avancement des Premières Nations vers la souveraineté des données.

Clinical and Laboratory Standards Institute (CLSI)	Le CLSI est un organisme sans but lucratif américain qui élabore et publie des normes consensuelles pour le secteur de la santé. Il compte parmi ses membres plus de 1 400 organisations et 400 personnes de 60 différents pays. Le CLSI est actif au sein de l'ISO et assure le secrétariat du comité technique ISO/TC 212 sur les laboratoires de biologie médicale et systèmes de diagnostic in vitro.
COMITÉS DE L'American National Standards INSTITUTE (ANSI)	L'ANSI est un organisme sans but lucratif privé qui promeut et facilite l'élaboration de normes volontaires et consensuelles (produits, services, processus, systèmes et personnel) et de systèmes d'évaluation de la conformité aux États-Unis. Chef de file parmi les grandes organisations de normalisation et d'accréditation mondiales et régionales, l'ANSI est le seul représentant américain à l'ISO, et à l'IEC par l'entremise du United States National Committee.
Commission électrotechnique internationale (IEC)	La Commission électrotechnique internationale est une organisation internationale de normalisation qui prépare et publie des normes internationales sur toutes les technologies de l'électricité, de l'électronique et des domaines connexes. L'IEC compte de nombreux comités techniques conjoints avec l'ISO, notamment l'ISO/IEC JTC 1.
Commission Internationale de l'Éclairage (CIE)	La CIE est une organisation vouée à l'échange d'informations et à la coopération entre les pays membres sur les questions concernant la science et l'art de l'éclairage. Considérée comme une autorité internationale en matière de lumière, de couleur d'éclairage et d'espaces chromatiques, la CIE publie des normes sur la science et l'art de la lumière et de l'éclairage, de la couleur et de la vision, de la photobiologie et de la technologie de l'image.
Conseil d'identification et d'authentification numériques du Canada (CCIAN)	Le CCIAN est une coalition canadienne à but non lucratif d'organisations privées et publiques qui œuvre à mettre au point un cadre canadien d'identification et d'authentification numériques. Il a publié le Cadre de confiance pancanadien (CCP) – un ensemble de normes d'identification et d'authentification numériques – pour aider les entreprises et les gouvernements à créer des outils et des services tout en favorisant l'interopérabilité, l'expérience utilisateur, la confidentialité, la sécurité et la convivialité. Le CCIAN compte trois comités, dont le Comité d'experts du cadre de confiance, qui a préparé le CCP et élabore des normes et des documents connexes pour assurer l'interopérabilité des services d'identité. Le CCIAN a contribué à fonder le Laboratoire d'identité numérique du Canada, qui propose des services d'évaluation, de mise à l'essai et de certification de la conformité et de l'interopérabilité pour les solutions d'identité numérique.
Conseil stratégique des DPI (CSDPI)	Le CSDPI est un organisme d'élaboration de normes canadien accrédité par le CCN. Il se concentre surtout sur les technologies émergentes dans le secteur des technologies de l'information et des communications (TIC) au Canada. Il a publié des normes sur la gouvernance des données, la confiance et l'identité numérique, et l'intelligence artificielle. Voici quelques-uns de ses groupes de travail : • TC 1 : Gouvernance des données • TC 4 : Confiance et identité numérique • TC 10 : Systèmes bancaires ouverts

Consortium World Wide Web (W3C)	Le W3C est l'un des principaux organismes de normalisation internationaux pour le World Wide Web. Il compte plusieurs groupes de travail qui œuvrent à l'élaboration de normes liées à l'identité numérique, aux identifiants et à l'authentification : • groupe de travail sur les identifiants vérifiables; • groupe de travail sur les identifiants décentralisés; • groupe de travail sur la sécurité des applications Web; • groupe de travail sur l'authentification sur le Web. Le W3C compte également plusieurs groupes d'intervenants qui ne rédigent pas de normes, mais publient des rapports sur divers sujets : • groupe d'intervenants sur les identifiants; • groupe d'intervenants sur l'identification numérique; • groupe d'intervenants sur la vérification numérique; • groupe d'intervenants sur l'identification des utilisateurs sur le Web.
DANISH Standards (DS)	DS est une organisation non gouvernementale privée et indépendante qui agit à titre d'organisation nationale de normalisation au Danemark. DS propose des services de normalisation dans divers domaines, de l'élaboration à la vente de normes et de publications associées. DS est membre de l'ISO, de l'IEC, du CEN, du CENELEC et de l'ETSI.
Decentralized Identity Foundation (DIF)	DIF est un groupe industriel qui promeut la mise en place de solutions d'identité décentralisée permettant aux entités de prendre le contrôle de leur identité et d'interagir en toute confiance. Il appuie, à l'échelle sectorielle, les discussions et les contributions au code source libre, et encourage l'interopérabilité. Le groupe travaille à divers projets, notamment un résolveur universel, un registre universel et une méthode pour les identifiants décentralisés entre pairs. La direction du groupe compte surtout des Américains, mais les autres pays y sont aussi représentés. Il compte parmi ses membres Microsoft, Hyperledger, Accenture, SecureKey et le ministère des Services aux citoyens de la Colombie-Britannique.
European Telecommunications Standards Institute (ETSI) **Comité Européen de Normalisation Électrotechnique (CENELEC)** **Comité Européen de Normalisation (CEN)**	L'ETSI, le CENELEC et le CEN sont les trois organismes de normalisation officiellement reconnus par l'Union européenne. L'ETSI est l'organisme de normalisation officiel pour les TIC, les télécommunications, la radiodiffusion et les autres réseaux de communication électronique; le CENELEC s'occupe du génie électrique et électrotechnique, et le CEN, de tous les autres domaines techniques. Deux comités techniques pertinents relèvent conjointement du CEN et du CENELEC, et un du CEN : • le CEN/CTC/JTC 13 sur la cybersécurité et la protection des données; • le CEN/CTC/JTC 19 sur les chaînes de blocs et technologies de registre distribué; • le CEN/TC 224 sur l'identification des personnes et dispositifs à caractère personnel associés, comprenant élément de sécurité, systèmes, opérations et données privées sécurisés dans un environnement multisectoriel. Mentionnons la famille de normes ISO/IEC 27000 relative à la sécurité de l'information. Certaines d'entre elles ont d'abord été publiées par le CEN et le CENELEC avant d'être adoptées par l'ISO.
Financial Data Exchange (FDX)	FDX est un organisme sans but lucratif américain qui promeut l'adoption généralisée d'une norme commune, interopérable et libre de droits pour l'accès sécurisé à des données financières autorisées par l'utilisateur, appelée FDX API. Il compte des membres de nombreux pays qui font la promotion des principes de l'échange de données autorisées par l'utilisateur, dont des institutions financières, des agrégateurs de données financières, des entreprises de technologie financière, des réseaux de paiement, des groupes de consommateurs, des groupes et des services du secteur financier et d'autres parties autorisées de l'écosystème des données financières autorisées par l'utilisateur. Situé aux États-Unis, FDX a récemment lancé un groupe de travail canadien qui compte 31 organisations du secteur financier du Canada, dont BMO, CIBC, Desjardins, la Banque Équitable, Flinks, Interac, Intuit, Mastercard, la Banque Nationale, RBC, la Banque Scotia, SecureKey et TD. Le groupe de travail canadien est représenté au conseil d'administration de FDX par RBC et Interac (cette dernière étant une initiative de coopération lancée en 1984 par RBC, CIBC, Banque Scotia, TD et Desjardins).

Fondation OpenID (OIDF)	La fondation OpenID est un organisme de normalisation international sans but lucratif composé d'individus et d'entreprises déterminés à favoriser, promouvoir et protéger les technologies OpenID. Elle agit comme organisation de fiducie d'intérêt public représentant la communauté des développeurs, des vendeurs et des utilisateurs, qu'elle aide en fournissant l'infrastructure nécessaire ainsi qu'en promouvant et appuyant l'adoption généralisée des normes OpenID. La fondation a publié Open ID Connect 1.0, une couche d'identification qui se superpose au protocole OAuth 2.0 pour permettre au client de vérifier l'identité d'un utilisateur final à partir de l'authentification réalisée par un serveur d'autorisation, et d'obtenir le profil de base de cet utilisateur. La fondation OpenID compte plusieurs groupes de travail qui se penchent notamment sur les sujets suivants : • Profil d'authentification amélioré; • eKYC et assurance de l'identité; • Profil international d'assurance de l'identité auprès des services publics. Elle compte parmi ses commanditaires Google, Microsoft et Verizon, et parmi ses nombreux membres, Amazon Web Services (AWS), Deutsche Telekom, eBay, Intuit et PayPal.
German Institute for Standardization (DIN)	Le DIN est l'organisme national de normalisation qui représente l'Allemagne à l'ISO. Il élabore des normes sur la rationalisation, l'assurance qualité, la protection de l'environnement, la sécurité et la communication dans divers domaines : technologie, science, industrie, administration publique et secteur public.
Groupe CSA (CSA)	Le CSA est un organisme d'élaboration de normes canadien accrédité par le CCN. C'est l'un des plus grands organismes d'élaboration de normes en Amérique du Nord; il compte aussi des bureaux en Europe et en Asie. Les activités de normalisation du CSA couvrent un éventail de domaines, dont la construction, l'énergie, la santé, les TIC et le transport. C'est le CSA qui a publié les versions canadiennes d'un grand nombre de normes ISO liées aux TI et à la cybersécurité, entre autres.
Hyperledger	Hyperledger est une communauté ouverte qui élabore une série de cadres, d'outils et de bibliothèques stables pour le déploiement de chaînes de blocs à l'échelle organisationnelle. Il s'agit d'une collaboration internationale hébergée par la Fondation Linux qui regroupe des leaders de la finance, des banques, de l'Internet des objets, des chaînes d'approvisionnement, de la fabrication et de la technologie. Elle compte parmi ses membres IBM, Hitachi, J. P. Morgan, American Express, Digital Asset (DAML), FedEx, Huawei, Lenovo, R3, Red Hat, Ripple, SAP, SecureKey, Walmart, entre autres. La Bank of England, la DIF, GS1, le gouvernement de la Colombie-Britannique, la Fondation Sovrin, l'Université Yale se trouvent parmi les membres associés. L'initiative compte divers projets en code ouvert, dont notamment : • Aries – infrastructure d'interaction entre pairs basée sur les chaînes de blocs qui constitue une trousse à outils partagée, réutilisable et interopérable conçue pour les initiatives et les solutions de création, de transmission et de conservation des identifiants numériques vérifiables. • Indy – registre distribué conçu spécialement pour les identités décentralisées. • Ursa – bibliothèque cryptographique partagée qui permet aux personnes (et aux projets) d'éviter de dédoubler les travaux cryptographiques d'un projet à l'autre, améliorant ainsi la sécurité.
Initiative Kantara	L'Initiative Kantara est une association professionnelle américaine sans but lucratif qui propose aux fournisseurs de services des ressources en matière d'évaluation de la conformité et d'approbation de l'assurance en vertu de la catégorie d'approbation NIST 800-63-3 de son cadre d'assurance des justificatifs d'identité. Elle élabore également des spécifications qu'elle soumet aux organismes de normalisation officiels pour répondre aux nouveaux besoins de l'industrie et du marché. Elle compte parmi ses membres des entreprises d'Amérique du Nord, d'Europe et d'Océanie, dont Experian, Idemia, digi.me, Identos, et Mastercard. Elle a également des contacts ou des ententes de partenariat avec des organisations comme DID Alliance, Digital Identity New Zealand, Financial Data Exchange, l'Alliance FIDO, l'European Association for e-Identity and Security, et le Conseil d'identification et d'authentification numériques du Canada (CCIAN).

Institute of Electrical and Electronics Engineers (IEEE)	L'IEEE est une association de professionnels en génie électronique, en génie électrique et dans les disciplines connexes. Elle s'occupe également de la normalisation dans une vaste gamme de domaines liés au génie et à l'informatique. L'association est structurée en plusieurs comités, communautés, sociétés, conseils techniques, communautés techniques et groupes de travail, selon l'expertise et la spécialisation.
Internet Engineering Task Force (IETF)	L'IETF est un organisme de normalisation ouvert, qualifié par certains de « chef de file des normes sur Internet ». Il élabore des normes volontaires sur Internet, notamment celles qui composent la suite de protocoles Internet (TCP/IP). Il compte notamment le groupe de travail OAuth, qui a mis au point le protocole du même nom.
Internet Society	L'Internet Society est un organisme sans but lucratif américain regroupant des membres du monde entier qui travaillent ensemble pour « développer et renforcer l'Internet ». Il favorise l'accessibilité à Internet, promeut le développement et l'application de son infrastructure, de ses technologies et de ses normes ouvertes, et assure un leadership quant aux politiques du domaine. L'organisme milite pour une approche décentralisée du fonctionnement d'Internet et collabore avec des organisations du monde entier qui adhèrent aux mêmes principes. Il appuie l'élaboration ouverte de normes et protocoles, l'éducation dans les pays en développement, le perfectionnement professionnel et l'utilisation de forums de discussion pour résoudre les problèmes, entre autres. Il compte parmi ses membres des entreprises comme Comcast, Amazon, AT&T, Google, Mozilla, le CERN, Facebook, LinkedIn, Nokia et Tencent.
Laboratoires des assureurs du Canada (ULC)	Normes ULC est accrédité par le CCN en tant qu'organisme de normalisation consensuelle dans le cadre du Système national de normes du Canada. ULC élabore et publie des normes et des spécifications de produits dans le domaine des incendies, de la sécurité des personnes, de la prévention du crime, de l'efficacité énergétique, de la sécurité environnementale, de la sécurité des biens et des installations, de la sécurité des travaux sous tension et de la sécurité au travail.
National Electrical Manufacturers Association (NEMA)	La NEMA est un organisme d'élaboration de normes accrédité par l'ANSI. Composée de chefs d'entreprise, d'experts en électricité, d'ingénieurs, de scientifiques et de techniciens, elle publie plus de 700 normes (sur l'électricité et l'imagerie médicale) et documents techniques couvrant des millions de produits de ses membres.
National Fire Protection Association (NFPA)	La NFPA élabore, publie et diffuse plus de 300 codes et normes consensuels visant à réduire au minimum les occurrences et les conséquences d'incendies et d'autres risques.
National Institute of Standards and Technology (NIST)	Le NIST est un laboratoire et un organisme non réglementaire du département du Commerce des États-Unis. Ses activités sont organisées en programmes expérimentaux sur les nanosciences et nanotechnologies, le génie, les technologies de l'information, les neutrons, la mesure des matériaux et le mesurage physique.
OASIS Open	OASIS est un organisme de normalisation sans but lucratif qui encourage l'élaboration juste et transparente de normes et de logiciels en code ouvert grâce au mouvement collectif et à la collaboration internationales. Les membres d'OASIS œuvrent à des projets sur la cybersécurité, les chaînes de blocs, l'Internet des objets, les interventions d'urgence, l'infonuagique, l'échange de données juridiques et bien davantage. OASIS participe également à l'élaboration de normes nationales au sein de l'ISO, par l'intermédiaire de l'organisme de normalisation américain ANSI. Il est notamment actif dans le comité de projet ISO/PC 317 (Protection des consommateurs : respect de la vie privée assuré dès la conception des biens de consommation et services aux consommateurs) et le comité technique ISO/TC 324 (Économie du partage). IBM a commandité la création de cet organisme, qui compte également une longue liste de contributeurs et de commanditaires dont Adobe, Cisco, Dell, HP, Huawei, McAfee, Microsoft, Red Hat, TELUS, le département de la Défense américain, la Bank of America, la Fondation Ethereum, Google et Boeing.

Office des normes générales du Canada (ONGC)	L'ONGC est une organisation gouvernementale fédérale axée sur les besoins du client, qui propose des services exhaustifs de normalisation et d'évaluation de la conformité pour servir les intérêts de ses partenaires dans les domaines de l'économie, de l'approvisionnement, de la santé, de la sécurité et de l'environnement. L'ONGC est accrédité par le CCN en tant qu'OEN, organisme de certification de produits et organisme de certification de systèmes de management.
Open Banking Initiative Canada (OBIC)	L'OBIC, une organisation qui représente le secteur des services financiers (consommateurs, entreprises de technologie financière, banques et experts du secteur), travaille à lancer et à diriger la création d'un cadre de services bancaires ouverts au Canada. L'écosystème ainsi formé évaluera la technologie et les normes visant l'instauration d'un climat de confiance entre les entreprises de technologie financière, les banques et les autorités de réglementation canadiennes. Le conseil d'administration d'OBIC compte des représentants de Wealthsimple, Axway, The AML Shop, la Large Credit Union Coalition et l'Association canadienne des coopératives financières.
Organisation internationale de normalisation (ISO)	L'ISO est le plus grand organisme de normalisation indépendant, international et non gouvernemental. Comptant 165 organismes de normalisation nationaux, il rassemble des experts pour élaborer des normes volontaires et consensuelles. Il a contribué à l'élaboration de diverses normes sur les technologies de l'information, dirigées notamment par un comité technique, l'ISO/IEC JTC 1 – Technologies de l'information, et plusieurs de ses sous-comités, principalement : • ISO/IEC JTC 1/SC 17 – Cartes et dispositifs de sécurité pour l'identification des personnes; • ISO/IEC JTC 1/SC 27 – Sécurité de l'information, cybersécurité et protection de la vie privée; • ISO/IEC JTC 1/SC 31 – Techniques automatiques d'identification et de saisie de données; • ISO/IEC JTC 1/SC 32 – Gestion et échange de données.
SAE International (SAE)	SAE est un organisme de normalisation américain qui s'adresse aux ingénieurs. Ses normes font évoluer le génie des transports partout dans le monde. Il propose aux secteurs qu'il vise – aérospatiale, automobile et véhicules commerciaux – différents services, notamment son programme de normalisation technique.
Standards New Zealand (SNZ)	Organisme de normalisation national de la Nouvelle-Zélande, SNZ fait partie du ministère des Affaires, de l'Innovation et de l'Emploi. Il gère notamment l'élaboration des normes en plus de publier et de vendre des normes néo-zélandaises, des normes élaborées conjointement par l'Australie et la Nouvelle-Zélande, et des normes internationales.
Union internationale des télécommunications – Secteur de la normalisation des télécommunications (UIT-T)	L'UIT-T est l'un des trois secteurs de l'Union internationale des télécommunications (UIT), une institution spécialisée de l'Organisation des Nations Unies pour les technologies de l'information et des communications (TIC). Il coordonne les normes de télécommunications et de TIC et compte un certain nombre de commissions d'études et de groupes spécialisés. Mentionnons particulièrement la commission d'études 17 sur la sécurité et le groupe spécialisé sur l'application des technologies de registre distribué.
Union internationale des télécommunications – Secteur des Radiocommunications – Recommandations (UIT-R)	Les recommandations UIT-R forment un ensemble de normes internationales élaborées par le Secteur des radiocommunications de l'UIT. Ces recommandations sont approuvées par les états membres de l'UIT et élaborées par des experts d'administrations, d'exploitants, de l'industrie et d'autres organisations qui s'occupent de la radiocommunication partout dans le monde.

Annexe I –

Paysage normatif

SE REPÉRER DANS LE FICHIER EXCEL (télécharger le fichier)

L'index présente tous les mots clés associés aux 35 sujets. Cliquer sur un mot clé ou un sujet pour voir toutes les normes qui y sont associées.

Working Group / Groupe de travail	Focus Area (EN)	Secteur d'intérêt (FR)	Issue Number / Numéro de série	Issue Title (EN)	Titre du problème (FR)	Keywords/Subjects (EN)	Mots clés / sujets (FR)
WG1 / GT1	Foundations of Data Governance	Fondements de la gouvernance des	1	Accountability Framework	cadre d'imputabilité	Accountability Framework	cadre d'imputabilité
WG1 / GT1	Foundations of Data Governance	Fondements de la gouvernance des	1	Accountability Framework	cadre d'imputabilité	Accountability Framework and Liability	cadre d'imputabilité et responsabili
WG1 / GT1	Foundations of Data Governance	Fondements de la gouvernance des	1	Accountability Framework	cadre d'imputabilité	Accountability Model	modèle d'imputabilité
WG1 / GT1	Foundations of Data Governance	Fondements de la gouvernance des	1	Accountability Framework	cadre d'imputabilité	Accountability Tools	outils d'imputabilité
WG1 / GT1	Foundations of Data Governance	Fondements de la gouvernance des	1	Accountability Framework	cadre d'imputabilité	Consent and Accountability	consentement et imputabilité

Cliquer sur le mot clé pour voir les normes qui y sont associées

Les autres 35 feuilles présentent les normes associées à un sujet particulier. Un petit survol :

Triage fait par des bénévoles du groupe de travail

Numéro de la norme ou du document

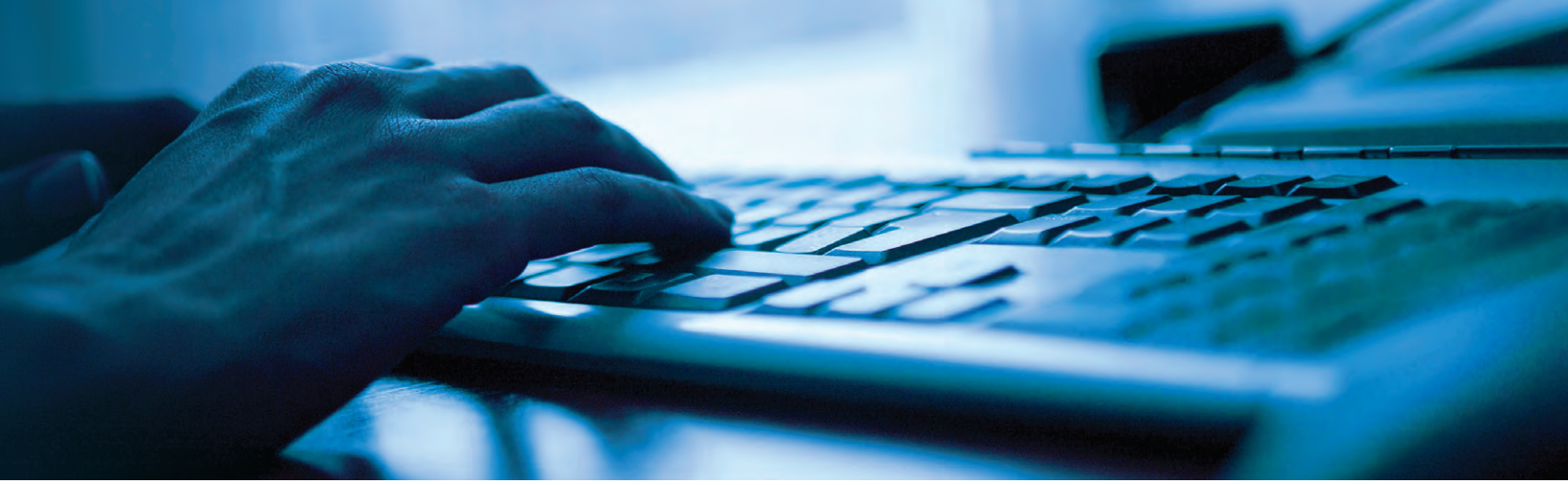
Région où la norme a été adoptée

Tier	English Title	French Title	ISEN	Publication Date	Publisher	Region (where the standard is published)	Adopted in	Keywords
I	Health informatics -	Informatique de santé -	ISO 11240	2012-11-01	ISO	International	Europe	Data traceability
I	Packaging – Bar code and two-	Emballage - codes à barres et	ISO 15394	2017-11-14	ISO	International	Europe	Data traceability
I	Information technology for	Technologies pour l'éducation,	ISO/IEC 20748.4	2020-02-28	ISO	International	Europe	Explicit consent & accountability
I	Information technology -	Technologies de l'information -	ISO/IEC 24760-2	2015-06-24	ISO	International	Europe	Explicit consent & accountability
I	Information technology —	Technologies de l'information -	ISO/IEC 29151	2017-09-30	ISO	International	Europe, Canada (CSA)	Explicit consent & accountability
I	Information technology -	Technologies de l'information -	ISO/IEC 29187-1	2013-03-01	ISO	International	Europe	Explicit consent & accountability
I	Information technology for	Technologies pour l'éducation,	ISO/IEC TS 20748-4	2019-09-30	ISO	International	Europe, Canada (CSA)	Explicit consent & accountability

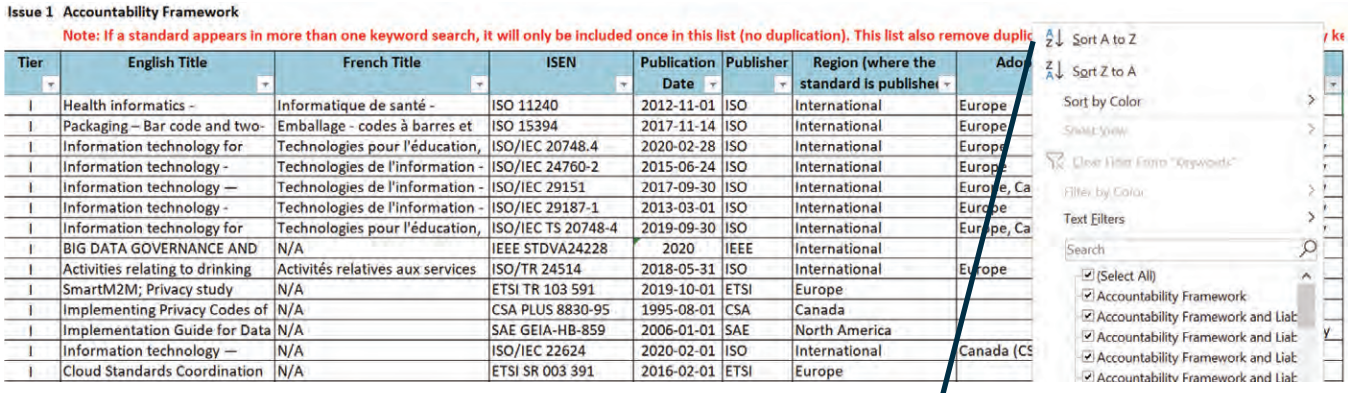
Nom de la norme en anglais et en français. Si la norme n'existe pas en français, le nom reste en anglais.

Organisme responsable (souvent un organisme d'élaboration de normes).

Mots clés pour faciliter les recherches. Une norme peut être associée à plusieurs mots clés.



Dans ces feuilles, vous pouvez trier les normes par titre, par numéro, par l'organisme responsable (p. ex., l'organisme d'élaboration de normes) ou par mot clé. Pour ce faire, choisir un des filtres.



Issue 1 Accountability Framework

Note: If a standard appears in more than one keyword search, it will only be included once in this list (no duplication). This list also remove duplic

Tier	English Title	French Title	ISEN	Publication Date	Publisher	Region (where the standard is publishe	Ado
I	Health informatics -	Informatique de santé -	ISO 11240	2012-11-01	ISO	International	Europe
I	Packaging – Bar code and two-	Emballage - codes à barres et	ISO 15394	2017-11-14	ISO	International	Europe
I	Information technology for	Technologies pour l'éducation,	ISO/IEC 20748.4	2020-02-28	ISO	International	Europe
I	Information technology -	Technologies de l'information -	ISO/IEC 24760-2	2015-06-24	ISO	International	Europe
I	Information technology —	Technologies de l'information -	ISO/IEC 29151	2017-09-30	ISO	International	Europe, Ca
I	Information technology -	Technologies de l'information -	ISO/IEC 29187-1	2013-03-01	ISO	International	Europe
I	Information technology for	Technologies pour l'éducation,	ISO/IEC TS 20748-4	2019-09-30	ISO	International	Europe, Ca
I	BIG DATA GOVERNANCE AND	N/A	IEEE STDVA24228	2020	IEEE	International	
I	Activities relating to drinking	Activités relatives aux services	ISO/TR 24514	2018-05-31	ISO	International	Europe
I	SmartM2M; Privacy study	N/A	ETSI TR 103 591	2019-10-01	ETSI	Europe	
I	Implementing Privacy Codes of	N/A	CSA PLUS 8830-95	1995-08-01	CSA	Canada	
I	Implementation Guide for Data	N/A	SAE GEIA-HB-859	2006-01-01	SAE	North America	
I	Information technology —	N/A	ISO/IEC 22624	2020-02-01	ISO	International	Canada (CS
I	Cloud Standards Coordination	N/A	ETSI SR 003 391	2016-02-01	ETSI	Europe	

Choisir un filtre pour afficher les normes qui vous intéressent.