



Rapport exécutif des conseils mixtes sur les tendances ce mois-ci

L'innovation gouvernementale, le rôle du dirigeant principal de l'information (DPI) et l'intelligence artificielle (IA) au gouvernement étaient les tendances clés de ce mois-ci.

Points clés – Innovation gouvernementale



Royaume-Uni – Le gouvernement du Royaume-Uni a dévoilé sa stratégie sur l'innovation grandement anticipée, laquelle établit l'approche nationale à la numérisation du secteur public. La [Government Technology Innovation Strategy](#), lancée le 10 juin, présente les propositions sous les thèmes des personnes; des processus; et des données et de la technologie. Elle indique également les façons dont le gouvernement peut améliorer la coordination et la cohésion entourant l'innovation au moyen de consultations menées dans les secteurs public et privé et dans le milieu universitaire.

Quelques faits saillants :

- L'élan vers les détachements se démarque comme l'initiative la plus notable dans la section sur les 'personnes' de la stratégie. On demande au gouvernement d'explorer

le l'adaptation, le changement, le développement des principaux dirigeants de la fonction publique dans l'industrie afin de leur permettre d'être témoins des bénéfices d'une culture d'expérimentation et d'adopter ces pratiques lorsqu'ils retournent au gouvernement.

- Le segment sur les 'processus' de la stratégie se concentre sur les progrès réalisés avec la création récente du marché Spark de 650 M£ du gouvernement : un système d'achat dynamique couvrant 64 types de technologies dans divers secteurs visant à améliorer l'adoption de la technologie.
- La section sur les données et la technologie met en lumière le plan d'élaborer une perspective intergouvernementale détaillée de l'étendue du défi de la technologie héritée, de mettre en place des plans pour le relever et de veiller à ce que des améliorations soient continuellement réalisées dans son patrimoine technologique.

Hong Kong – Un laboratoire de l'innovation pour un gouvernement intelligent a été lancé à Hong Kong dans le but d'appuyer les petites et moyennes entreprises technologiques et les entreprises de démarrages avec le développement de produits qui peuvent améliorer les services publics. Le laboratoire travaillera également à sensibiliser l'administration de Hong Kong aux technologies qui pourraient être utiles aux fonctionnaires. [En savoir plus ici.](#)

Points clés – Dirigeants principaux de l'information



États-Unis – [GovTech a recueilli les données de 206 mandats de DPI d'États](#)

remontant jusqu'à 1994 afin d'en apprendre plus au sujet des personnes chargées de la technologie dans le gouvernement des États.

Voici quelques faits saillants :

- le poste précédent de cinquante-neuf pour cent des DPI d'États était dans la fonction publique;
- après avoir servi comme DPI d'États, 52 pour cent de ce groupe se déplaçait au secteur privé;
- les DPI demeuraient en poste pour une période de trois ans et six mois en moyenne.

États-Unis – [Un récent article](#) sur les compétences dont les DPI gouvernementaux ont besoin affirmait que le rôle en évolution des DPI représente ce qui s'est produit à plus grande échelle dans la TI des gouvernements. L'ère de la virtualisation, de la construction de centres de données et de l'efficacité opérationnelle en général s'estompe. La transition de la technologie au consumérisme de masse a transformé le rôle de TI de sa fonction administrative principale, servant les travailleurs du gouvernement, en une fonction qui devrait habiliter un large éventail de nouveaux services qui peuvent être téléchargés sur des téléphones intelligents et fournir aux citoyens des expériences personnalisées.

États-Unis – Dans un récent article et une vidéo de GovTech, le DPI Jim Weaver [explique](#)

[l'importance d'une bonne gouvernance, de processus opérationnels reproductibles et de la mise en œuvre de Microsoft Office 365](#) qui formeront une première étape essentielle vers l'efficacité généralisée.

Points clés – Intelligence artificielle



Canada – [traduction] « Afin d'assurer la prospérité de l'IA au Canada, il est critique que la politique publique soit la bonne pour trois piliers clés : générer de la croissance dans une économie dirigée par l'IA, accroître le bien public et accroître la confiance dans les institutions et la société », [Deloitte a indiqué dans un rapport sur l'IA](#). Pourtant, seulement quatre pourcent des Canadiens sondés par Deloitte ont affirmé qu'ils étaient confiants dans leur compréhension de l'IA. Selon le rapport, un autre obstacle qui ralentit la croissance de l'IA est la méfiance des Canadiens envers la technologie.

Estonie – Le dirigeant principal des données de l'Estonie est en mission pour mettre en œuvre l'IA dans tous les aspects des services publics de pays, des soins de santé à l'éducation et aux centres d'emploi. [Apprenez-en plus](#) au sujet de la vision du dirigeant principal des données pour l'avenir et les premières réussites réalisées jusqu'à maintenant.

États-Unis – Dépassés par les alertes et contraints par des ressources limitées, les gouvernements d'État ont besoin d'un nouveau plan pour lutter contre les menaces et les attaques numériques. L'IA pourrait être la réponse, puisqu'elle offre la promesse d'analyser

de larges volumes d'événements de sécurité, augmentant la chance que les menaces réelles soient détectées plus rapidement. [Apprenez-en plus](#) au sujet des capacités défensives et des défis potentiels associés à l'utilisation de l'IA pour la cybersécurité au niveau des États.

Royaume-Uni – Le 10 juin, le [gouvernement du Royaume-Uni a annoncé](#) un investissement maximal de 18,5 M£ afin d'appuyer les efforts visant à accroître la diversité dans les rôles des sciences de l'IA et des données en offrant des diplômes de conversion, des bourses d'études pour les groupes sous-représentés et des possibilités d'apprentissage en ligne.

Autres articles dignes de mention sur l'IA

[Chien de garde indépendant clé à la surveillance de l'intelligence artificielle](#), University World News

Autres articles dignes de mention ce mois-ci

[Clients mécontents : les services publics inhumains brisent-ils les liens de confiance?](#), The Mandarin

[Le budget de Queensland investit 85 millions de dollars dans les services numériques et la cybersécurité](#), IT News

[Les jumeaux numériques municipaux peuvent transformer la planification des villes](#), Forbes

[Exclusif : Comment la technologie émergente influencera le secteur public](#), IT Brief

[L'Illinois lance un portail pour simplifier les services fiscaux locaux](#), Government Technology

[Changer la face du gouvernement normal au moyen de la transformation numérique](#), Open Access Government

[Votre administration devrait-elle avoir un groupe Facebook?](#), Government Technology [en anglais seulement]

Répertoire de recherche

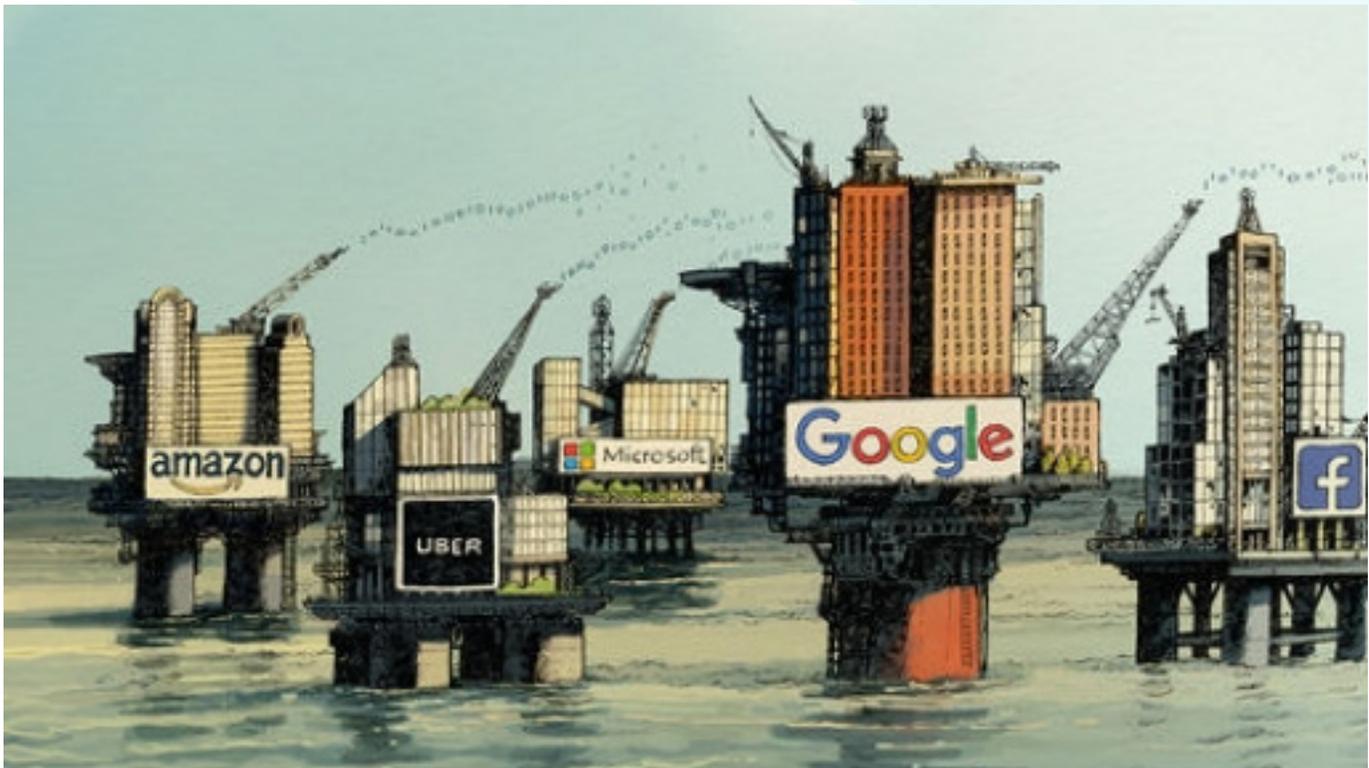
□ Consultez le répertoire de recherche de l'Institut des services axés sur les citoyens (ISAC) [ici](#).

Le nouveau contenu comprend les articles suivants : What governments need to be truly citizen-centric; Big Data and Artificial Intelligence — The Future of Accounting and Finance; Ten years on: What's next for behavioural insights?

Protection de la vie privée ou « Demandez-le-moi une seule fois » – Devons-nous choisir?



En 2017, The Economist a déclaré que « [la ressource la plus précieuse du monde n'est plus le pétrole, mais les données.](#) »



Les données personnelles sont maintenant une grande affaire. Selon [un article de 2018 du New Yorker](#) :

[traduction] « Nous nous abonnons pour recevoir un service, mais nous ne pensons pas vraiment à qui pourrait stocker nos clics ou ce qu'ils font avec nos renseignements personnels. C'est étrange au départ lorsque nos appareils semblent 'savoir' où nous habitons, notre âge, les livres que nous aimons ou la marque de dentifrice que nous utilisons. Puis nous nous habituons à cette familiarité et commençons même à en être reconnaissants. Cela fait que le monde en ligne nous semble personnalisé pour nous et réduit le temps nécessaire pour tracer le chemin jusqu'à chez soi ou commander quelque chose de nouveau à lire. La machine anticipe ce que nous voulons, mais... nous ne savons pas réellement qui voit nos données ou comment ils les utilisent. »

En réponse à l'enjeu des données utilisées de manières dont les gens ne sont pas conscients, certains pays ont pris la position de protéger la vie privée et les données personnelles des citoyens.

Les mesures législatives du RGPD¹ sont considérées comme la référence en matière de protection de la vie privée. Selon le [Raconteur](#), la raison est qu'en vertu des [exigences strictes du RGPD](#), toute entreprise mondiale qui vend aux consommateurs de l'Union européenne ou qui les cible doit se conformer aux nouvelles mesures législatives, peu importe l'endroit où cette entreprise est établie.

¹ Règlement général sur la protection des données : un règlement dans le cadre législatif de l'Union européenne sur la protection des données et de la vie privée de tous les citoyens de l'Union européenne et de l'Espace économique européen.

L'UE fait essentiellement du RGPD une référence mondiale pour la réglementation en matière de protection de la vie privée.

Le tableau suivant² offre un guide rapide concernant les lois en matière de protection de la vie privée de certaines administrations qui sont également reconnues pour avoir une bonne prestation de services; il a été élaboré au moyen des données fournies par [i-Sight](#) et la [Commission européenne](#), soulignant que les lois en matière de protection de la vie privée au Danemark et au Royaume-Uni devraient être conformes au RGPD.

Pays	Canada	Danemark (UE)	Australie	Royaume-Uni (UE)
Protection suffisante selon le RGPD?	Oui (organisations commerciales; gouverné par la Loi sur la protection des renseignements personnels et les documents électroniques [LPRPDE]; voir ci-dessous)	Oui	Non	Oui
Lois en matière de protection de la vie privée	<p>Le Canada a 28 lois fédérales, provinciales ou territoriales qui gouvernent la protection des données et de la vie privée dans le pays.</p> <p>Au niveau national, la collecte, l'utilisation et la divulgation de renseignements personnels dans le secteur privé sont gouvernées par la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) de 2000. La PRPDE a été modifiée pour la</p>	<p>Les mesures de protection de la vie privée au Danemark sont réglementées par la Loi danoise de 2018 sur la protection des données (loi no 502 du 23 mai 2018), anciennement la Loi danoise sur le traitement des données personnelles (loi no 429 du 31 mai 2000).</p> <p>Cette nouvelle loi sur la protection des données complète le Règlement général sur la protection des données (2016/679) (à titre d'information : les pays de l'UE ont</p>	<p>La Privacy Act de 1988 de l'Australie est la principale loi sur la protection de la vie privée qui gouverne à la fois les secteurs public et privé.</p> <p>La Privacy Act est fondée sur 13 principes australiens de protection de la vie privée qui couvrent la transparence et l'anonymat; la collecte, l'utilisation et la divulgation de données; le maintien de la qualité des données; et les droits des personnes concernées.</p>	<p>Le Royaume-Uni est présentement assujéti à la Data Protection Act de 2018, laquelle comporte le RGPD de l'UE et complète ses dispositions.</p> <p>La Data Protection Act de 2018 se concentre principalement sur les droits des personnes concernées; les données personnelles de catégorie spéciale; les frais liés à la protection des données; les infractions à la protection des données; le consentement des enfants; et l'application</p>

² Les pays comparés ont été sélectionnés puisque l'on considère que leurs secteurs publics offrent d'excellents services numériques.

Pays	Canada	Danemark (UE)	Australie	Royaume-Uni (UE)
	<p>dernière fois en novembre 2018 afin d'inclure des mesures législatives de signalement obligatoire des fuites de données et de conservation des renseignements. Pour le secteur public, comme les ministères fédéraux et les sociétés d'État, la protection des données personnelles est gouvernée par la Loi sur la protection des renseignements personnels de 1983.</p> <p>Les provinces et les territoires ont chacun leurs propres mesures législatives du secteur public. Par exemple, l'Alberta est gouvernée par la Personal Information Protection Act (PIPA) de 2004. La Colombie-Britannique est gouvernée par une loi portant le même nom qui est entrée en vigueur un an plus tôt. L'Ontario a également sa propre loi sur la protection des renseignements personnels, la Loi de 2004 sur la protection des renseignements personnels sur la santé.</p>	<p>l'obligation de mettre à jour ou d'adopter leurs propres lois fédérales sur la protection de la vie privée de manière à correspondre aux dispositions du RGPD).</p> <p>La Loi danoise de 2018 sur la protection des données comporte des dispositions concernant le traitement des données, la divulgation des données personnelles, le droit d'accès, la désignation d'un délégué à la protection des données, les limites au consentement, les interdictions sur le transfert de données, les sanctions administratives et plus.</p>	<p>En plus de la Privacy Act fédérale de 1988, la protection des données est gouvernée par des mesures législatives de protection de la vie privée (dans la majorité des États australiens) et de lois sur la protection de la vie privée propres aux secteurs (selon les données en question).</p> <p>Par exemple, les organisations qui recueillent, utilisent ou divulguent des données sur la santé sont gouvernées par des principes distincts de protection des renseignements sur la santé. Les organisations à Queensland qui traitent des données personnelles sont également gouvernées par la Information Privacy Act de 2009.</p>	<p>de la loi.</p> <p>Le Royaume-Uni ne sera plus un État membre de l'UE à compter du 31 octobre 2019. Toutefois, il n'y a eu aucune indication que le Royaume-Uni changera ses lois existantes sur la protection des renseignements personnels.</p>

Pays	Canada	Danemark (UE)	Australie	Royaume-Uni (UE)
Pour en savoir plus	<ul style="list-style-type: none"> • Site Web du gouvernement • LPRPDE 2000 • Modifications de 2018 de la LPRPDE • Loi sur la protection des renseignements personnels de 1983 • PIPA 2004 d'Alberta • PIPA 2003 de la Colombie-Britannique • LPRPS 2004 	<ul style="list-style-type: none"> • Site Web du gouvernement • Loi danoise de 2018 sur la protection des données • Règlement général sur la protection des données de 2016 	<ul style="list-style-type: none"> • Site Web du gouvernement • Federal Privacy Act 1988 • Principes de protection de la vie privée • Information Privacy Act 2009 	<ul style="list-style-type: none"> • Site Web du gouvernement • Data Protection Act 2018

La protection de la vie privée est importante : Perspectives des Canadiens concernant la protection des renseignements personnels

La protection de la vie privée est importante pour les Canadiens



La protection des renseignements personnels et la sécurité ont toujours été des concepts importants pour les gens au Canada. Dans le [rapport Canada Next d'Ipsos](#) (2017), il est indiqué que trois quarts des Canadiens croient que les citoyens devraient être les détenteurs des données recueillies à leur sujet par les gouvernements et 72 % sont d'accord que les données générées par les Canadiens devraient être protégées et réglementées de manière semblable aux ressources naturelles.

Ipsos indique également que 69 % des Canadiens sont d'accord que, lorsqu'ils pensent au sujet des avancées futures de la technologie, ils sont très préoccupés au sujet de la confidentialité et de la sécurité de leurs renseignements personnels. Les Canadiens croient également que les données gouvernementales appartiennent aux citoyens (voir ci-dessous).

Les gouvernements au Canada respectent le fait que la protection de la vie privée est importante pour les Canadiens

Les Canadiens sont satisfaits de la façon dont les gouvernements au Canada respectent leur droit à la vie privée, comme le démontre la rétroaction fournie dans le rapport national « Les citoyens d'abord 8 ». Ce rapport affirme que les services gouvernementaux ont une bonne performance

pour la majorité des attributs de service, y compris l'équité, la protection de la vie privée, la communication (être informé de tout ce qu'il faut faire), les résultats et la satisfaction envers la voie de prestation.

Les Canadiens divulgueront des données afin d'obtenir un bon service selon IPSOS

Ipsos indique également que les Canadiens s'attendent à plus que le simple respect du droit à la vie privée. Ils veulent que les fournisseurs prennent les bonnes décisions quant à la façon de continuer à appuyer la protection de la vie privée tout en améliorant la prestation des services.

Cela doit-il être un champ de bataille? L'innovation contre la protection des renseignements?



Traditionnellement, il y a eu des tensions entre les possibilités que l'échange de renseignements crée pour améliorer l'expérience des services et la protection de la confidentialité des renseignements privés d'une personne. Il s'agit d'un problème qui existe depuis des années, où l'échange de renseignements personnels entre les organisations ou les administrations permet de demander « une seule fois » les renseignements personnels des personnes pour un large éventail de services. Bien que les personnes veuillent de la commodité, leur intérêt à fournir leurs données personnelles une seule fois et à ce qu'elles soient échangées entre les frontières n'est pas toujours préférable.

Ce conflit est communiqué dans le rapport [Government Information Sharing: Is Data Going Out of the Silos, Into the Mines?](#). Dans un article de 2018 du [Canadian Government Executive](#), il a été souligné que le rapport présentait des positions opposées : que tous les Canadiens veulent les bénéfices des services gouvernementaux électroniques et d'une réduction des fardeaux administratifs et que certains d'entre nous veulent également la protection de leur vie privée et de leur autonomie. Là repose le dilemme pour le secteur public.

Il n'est pas nécessaire qu'il y ait des tensions. La protection de la vie privée peut et devrait être intégrée aux services au fur et à mesure qu'ils sont conçus ou modifiés. Il s'agit de l'idée qui appuie le concept de « protection de la vie privée dès la conception ».

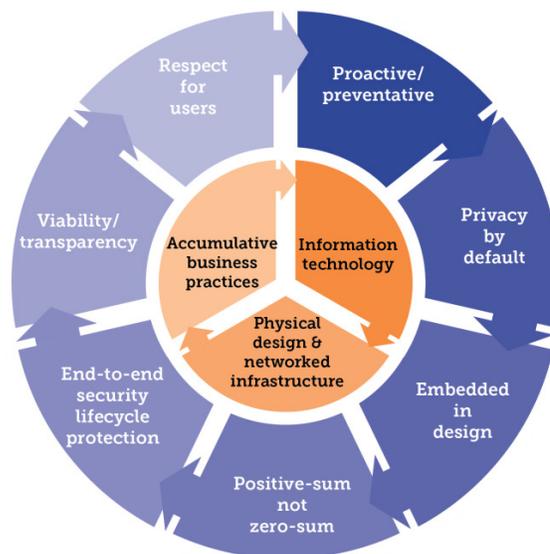
Protection de la vie privée dès la conception

La protection de la vie privée dès la conception est une approche particulière à la protection de la vie privée soutenue par l'ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario, [Mme Ann Cavoukian](#), initialement dans les années 1990, mais se poursuivant au cours des décennies subséquentes. Dans un [document de travail sur la protection de la vie privée dès la conception](#), la commissaire à la protection de la vie privée et des données (Australie) décrit la protection de la vie privée dès la conception comme une méthode qui permet d'intégrer

la protection de la vie privée dans la conception et l'architecture des systèmes d'information, des processus opérationnels et de l'infrastructure en réseau. La protection de la vie privée dès la conception vise à veiller à ce que la protection de la vie privée soit considérée à l'avance, au début et tout au long de l'élaboration et de la mise en œuvre d'initiatives qui comportent la collecte et le traitement de renseignements personnels.

Mme Cavoukian explique que, dans cette ère d'informatique répandue, de connectivité en ligne massive et de médias sociaux, nous ne serons jamais en mesure de régler contre toutes les atteintes à la vie privée si nous ne tentons pas de les prévenir dès le départ. Il n'est pas possible de le faire simplement avec les processus d'observation réglementaire après que les infractions aient eu lieu.

Le concept de protection de la vie privée dès la conception est fondé sur sept principes :



Cet [aide-mémoire](#) explique ces principes. Le [système eHealth](#) de l'Estonie, reconnue pour son travail dans le domaine du gouvernement numérique, offre un exemple pratique de la façon dont la protection de la vie privée dès la conception peut être appliquée. La Banque mondiale résume ce travail dans son rapport [Privacy by Design: Current practices in India, Estonia and Austria](#) comme suit :

[traduction] « *Consentement et choix des utilisateurs – Le système eHealth – Le cœur du système eHealth de l'Estonie est le système des dossiers de santé numériques, lequel utilise les formats de message HL7 et DICOM aux fins de l'interconnexion. La couche de transport et de sécurité des données est fournie par l'intergiciel X-Road. Les patients peuvent consulter toutes leurs données relatives aux soins de santé au moyen du portail des patients estoniens eHealth avec leur ID numérique pour confirmer leur identité. Par défaut, les spécialistes médicaux ont accès aux données, mais tout patient peut choisir de refuser l'accès aux fournisseurs de soins, y compris*

leurs propres omnipraticiens ou médecins de famille. D'autres, comme les pharmaciens et les assureurs, ont accès aux dossiers médicaux des patients, mais seulement avec la reconnaissance et le consentement explicites des patients. Toutes les demandes d'accès aux données dans le système sont enregistrées et les patients peuvent sur demande consulter ce registre. »

Il y a d'autres exemples de façons dont la protection de la vie privée dès la conception fonctionne en réalité qui ont été recueillis par la Banque mondiale dans le même rapport ici. D'autres ressources sur le sujet sont disponibles sur le [site Web Global Privacy by Design](#).

Nous serions ravis de vous entendre!

Nous aimerions connaître votre rétroaction!

Veillez cliquer sur le lien afin de répondre à trois questions simples.



[Prendre sondage](#)

Connaissez-vous quelqu'un qui souhaiterait consulter le rapport exécutif des conseils mixtes? Veuillez partager une copie de ce rapport. Si vous n'êtes pas encore abonné, vous pouvez vous inscrire pour obtenir des rapports exécutifs (mensuel) [ici](#) (vers fin de la page).

Envoyez vos questions à info@iccs-isac.org.