Deloitte.

Résoudre la crise de la gestion de l'identité dans le secteur public : il est temps que les gouvernements fassent preuve de sérieux en matière d'identité numérique

Il existe peut-être des outils pour résoudre la crise de la gestion de l'identité dans le secteur public, mais de réels progrès ne seront accomplis que si les gouvernements transforment considérablement leurs anciennes approches en matière d'identité numérique.

Toute personne qui se souvient d'avoir passé une demi-journée dans une file d'attente dans un service gouvernemental sait que d'énormes progrès ont été réalisés depuis quelques années. Aujourd'hui, environ 84 pour cent des pays donnent accès à leurs citoyens à au moins un service transactionnel en ligne et la moyenne mondiale s'établit à 14[1].

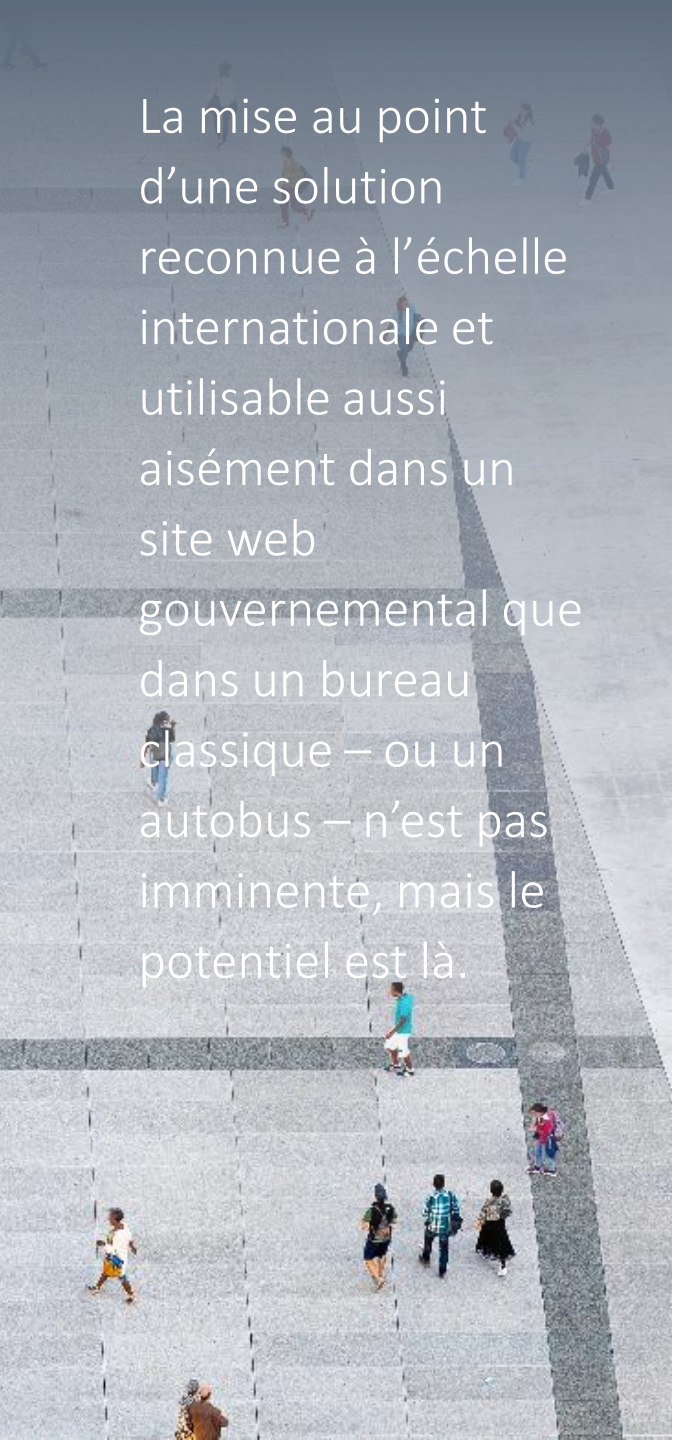
Pourtant, malgré ces avancées, il reste beaucoup à faire avant que les gouvernements puissent assurer la prestation de services entièrement numériques aux citoyens – pensons aux difficultés auxquelles ils ont fait face pour poursuivre leurs activités pendant la crise sanitaire. La technologie requise pour effectuer la transition vers les canaux numériques n'est pas en cause. Le problème, c'est que la plupart des gouvernements ne disposent pas des ressources, de la capacité, ni du savoir-faire nécessaires pour valider et protéger les identités numériques des citoyens.

Bien que la mobilisation suscitée par la pandémie ait vraisemblablement condensé 10 ans d'innovation numérique en 6 mois, le virage électronique des pouvoirs publics est pour le moins aléatoire. Pendant que d'innombrables organismes publics lançaient des initiatives isolées, les citoyens se sont fait offrir un méli-mélo de points d'accès, et ont dû créer des comptes d'utilisateurs exclusifs et se soumettre à de multiples strates de contrôle de la sécurité. Ce n'est pas juste une expérience utilisateur ingrate et laborieuse, c'est un cauchemar du point de vue de la cybersécurité.

Les chefs de l'information de l'ensemble des services gouvernementaux comprennent implicitement que les mots de passe à eux seuls procurent une protection insuffisante contre la cybercriminalité; à preuve, la prolifération de l'hameçonnage, des attaques de rançongiciels et de la fraude financière pendant la pandémie.

À défaut d'être dotés de systèmes de sécurité suffisamment résilients, les gouvernements ne peinent pas juste à protéger l'identité et les renseignements personnels des citoyens : ils sapent leurs propres efforts pour rendre accessibles avec un minimum de frictions leurs services essentiels. Il en résulte une expérience utilisateur médiocre pour les citoyens et l'enlisement des efforts de transformation numérique.

En clair, de nouvelles approches s'imposent.



Gouvernance, collaboration et contrôle par les utilisateurs

La refonte des méthodes de création, de sécurisation et d'utilisation des identités numériques amène les gouvernements à comprendre qu'ils doivent aller au-delà des solutions de base. Plutôt que de se borner à mettre au point des solutions permettant aux utilisateurs d'accéder plus facilement aux services en ligne – ce qui a pour effet de multiplier le cloisonnement des renseignements personnels sensibles et généralement mal protégés –, ils commencent à prendre conscience du véritable potentiel de l'identité numérique.

Par conséquent, la priorité se déplace des considérations entourant les moyens à prendre pour simplifier l'authentification vers des stratégies permettant la transmission numérique de données d'identification vérifiables en tout genre. Cette transition exige que les gouvernements réfléchissent plus sérieusement aux moyens à prendre pour réduire le stockage des renseignements des citoyens en habilitant ceux-ci à garder en leur possession et à contrôler eux-mêmes leurs renseignements personnels.

Un modèle en particulier, celui de l'identité autosouveraine (SSI), est en train de s'imposer en tant que candidat très prometteur pour l'infrastructure de l'identité numérique de l'avenir. Comme cette approche met l'accent sur des normes libres, une infrastructure ouverte et décentralisée et un modèle inversé de propriété des renseignements, elle se prête à l'utilisation d'identifiants réutilisables et vérifiables (pensons aux documents signés numériquement) qui peuvent être transmis directement aux portefeuilles d'identité mobiles des citoyens plutôt que de résider dans des bases de données centralisées des gouvernements ou de grandes sociétés technologiques.

Ce modèle habilite les citoyens à choisir quand et où communiquer leurs renseignements personnels tout en permettant aux destinataires de vérifier instantanément si le signataire d'un document numérique est digne de confiance.

La matérialisation de cette vision requiert cependant que les gouvernements créent un cadre de gouvernance rigoureux. Cela nécessite la clarification des responsabilités en matière de certification, d'authentification et de vérification des données d'identification numérique; la mise en place de règles et de directives connexes régissant la protection des renseignements; enfin, l'adoption des normes techniques nécessaires pour assurer la normalisation et l'interopérabilité des canaux, des secteurs d'activité et des frontières.

Par-dessus tout, les gouvernements devront reconnaître qu'ils ne peuvent relever seuls ce défi. Les dangers du recours à une approche émanant exclusivement du secteur privé en matière de validation de l'identité citoyenne et de gestion des renseignements personnels sont évidents, mais la participation du secteur privé sera indispensable non seulement pour définir collectivement des normes, mais également pour construire une infrastructure sécuritaire, conviviale, moderne et économiquement viable.

D'ores et déjà, un écosystème complexe de petits innovateurs en haute technologie, de grandes institutions financières, de fournisseurs de services de télécommunications et de géants de la technologie rivalisent d'ardeur pour être à l'avant-garde des solutions d'identité numérique de la prochaine génération. Ces organisations sont outillées pour mener à bien les initiatives gouvernementales, mais il incombe aux gouvernements de choisir judicieusement et d'élaborer la stratégie qui servira le mieux tant les citoyens que le secteur privé. À mesure que le centre de gravité se déplace des solutions sur place vers le nuage et les appareils de pointe comme les téléphones intelligents, la simplicité d'intégration des solutions de gestion de l'identité par l'intermédiaire de fournisseurs d'IaaS (identité en tant que service) et de services infonuagiques se généralise. Il incombe maintenant aux gouvernements de s'organiser et d'établir des partenariats collaboratifs avec le secteur privé.

Un potentiel à libérer

Il existe peut-être déjà des outils pour résoudre la crise de la gestion de l'identité dans le secteur public, mais de réels progrès ne pourront être accomplis que si les gouvernements perfectionnent considérablement leurs approches dépassées en matière d'identité numérique. Ceux qui relèveront ce défi ne se borneront pas à offrir à leurs citoyens un meilleur accès aux services gouvernementaux. Les gouvernements ont la possibilité d'ouvrir la voie à des niveaux inédits d'innovation dans leurs services, et ce, dans tous les secteurs de l'économie. Ils peuvent jeter des bases pour assurer la convergence des services, créer des modèles d'identité numérique interexploitables, et permettre aux citoyens de contrôler la manière de communiquer leurs renseignements personnels et les circonstances dans lesquelles ils le font.

Pour l'heure, la mise au point d'une solution reconnue à l'échelle internationale et utilisable aussi aisément dans un site web gouvernemental que dans un bureau classique – ou un autobus – n'est pas imminente, mais le potentiel est là. Les gouvernements doivent simplement être prêts à mettre ce potentiel en valeur.

1. Nations Unies, 2020, « E-Government Survey 2020 », https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf.

Personne-ressource

Amir Belkhelladi | Leader canadien, Cybersécurité
abelkhelladi@deloitte.ca