Principes d'une politique universelle sur l'identité numérique pour en optimiser les avantages pour les gens : une perspective européenne et canadienne commune

La place de l'humain dans un monde numérique

DIACC CCIAN

HUMAN TECHNOLOGY FOUNDATION

Introduction

Au 21e siècle, les décideurs du monde entier s'accordent à dire que la mise en place d'un écosystème permettant de vérifier l'identité des individus, en ligne et hors internet, est plus importante que jamais. Ce système doit être solide, fiable, respectueux de la vie privée et fondé sur des principes.

Durant la pandémie, l'exemple de l'application "TousAntiCovid", a montré l'importance de pouvoir s'appuyer sur une identité numérique protégeant les données, renforçant la maîtrise à l'utilisateur, et permettant une meilleure efficacité et précision des services. Cet écosystème est précieux en tant de crise, mais pas uniquement. Pour être performant, notre service de sécurité sociale dépend de plus en plus de données sûres et fiables. En outre, la mise en place de l'identité numérique est sans doute une condition préalable au développement d'un internet plus centré sur l'humain et à la concrétisation des "promesses" des technologies émergentes telles que le "Web3".

Une étude du Conseil canadien de l'authentification et de l'identification numérique (CCIAN) démontre que les Etats ont tout intérêt à réfléchir collectivement autour de la mise en œuvre de politiques et de technologies qui placent les utilisateurs - leurs avantages, leurs besoins et leurs préoccupations - au centre. Cela permettrait en effet un gain entre 3 et 13% du potentiel non réalisé de leur PIB , comme le confirme une étude de McKinsey. Ces deux études ont estimé la valeur potentielle à gagner en réduisant la fraude, en créant des gains d'efficacité et en équipant les services et entreprises de nouvelles méthodes d'identification.

Comme pour toute innovation, la réussite de ce projet passe par une co-construction des politiques publiques, avec comme lignes directrices la protection et la transparence.

https://diacc.ca/wp-content/uploads/2018/05/Economic-Impact-of-Digital-Identity-DIACC-v2.pdf
https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth

Notre objectif

La conception et la mise en œuvre optimales de politiques publiques liées à l'identité numérique sont au cœur de ce projet conjoint entre le Conseil Canadien de l'Authentification et de l'Identification Numérique (CCIAN) et la Human Technology Foundation (HTF). Le CCIAN est une coalition grandissante d'organisations des secteurs public et privé, qui font un effort considérable et soutenu pour assurer la participation totale, sûre et avantageuse du Canada à l'économie numérique mondiale. La Human Technology Foundation, créée en 2012, est une fondation mais aussi un réseau de recherche et d'action qui place l'être humain au cœur du développement technologique. Pour eux, ces technologies font aussi partie des solutions pour construire une société plus respectueuse de chacun. Le réseau de la Human Technology Foundation compte plusieurs milliers de membres et opère à Paris, Montréal et Genève.

Le but de ce rapport est de donner les clés aux décideurs qui définissent les politiques publiques relatives aux systèmes d'identification numérique. Nos recommandations font peser sur les organisations publiques et privées en charge du développement de l'identité numérique un devoir de diligence commun, afin d'assurer une mise en œuvre cohérente.

Ce rapport a été rédigé en plaçant l'humain au cœur des réflexions. Il est destiné aux décideurs publics et privés, ainsi qu'au grand public susceptible d'être intéressé par la conception des politiques publiques.

Les recommandations sont le fruit de l'analyse des dernières recherches et cas d'usages internationaux en matière d'identité numérique. HTF et CCIAN ont pour conviction que les gouvernements et les organisations du secteur privé doivent s'engager rapidement dans l'élaboration de politiques et intelligentes pour sécuriser et protéger les données relatives aux personnes et aux organisations. L'engagement public est également nécessaire pour promouvoir des solutions inclusives et équitables renforçant la confiance envers les écosystèmes numériques.

Le CCIAN et HTF espèrent que les décideurs des gouvernements nationaux et infranationaux, ainsi que les entités du secteur privé, utiliseront ce rapport comme un outil pour travailler avec toutes les parties prenantes : individus, aux entreprises, au secteur public et à la société civile.

Le concept d'identité numérique englobe des concepts complexes et une technologie sous-jacente, mais il s'agit avant tout d'un enjeu de

société. C'est pourquoi, nous avons choisi de simplifier au maximum les explications afin de se concentrer sur les impacts de ces technologies sur la société et chacun des utilisateurs (citoyen, entreprise, administration...). Afin de saisir les usages quotidiens liés à l'identité numérique, ce rapport utilise des scénarios basés sur des "persona". Au-delà d'identifier les opportunités liées à la mise en œuvre d'une identité numérique, nous avons identifié des recommandations qui nous semblent être des pré-requis pour que l'identité numérique soit acceptée et utilisée par les utilisateurs. De ce fait, le rapport n'a pas vocation à se prononcer sur les solutions ou les normes spécifiques relatives à la mise en œuvre de l'identité numérique, mais uniquement à identifier les principes clé pour que les projets d''identité numérique reposent sur un cadre de confiance.

Qu'est-ce que l'identité numérique?

Une extension de vous

L'identité numérique résulte d'une évolution des systèmes utilisés actuellement pour établir et confirmer l'identité des individus dans toutes sortes de contextes. En permettant d'identifier une personne en ligne et/ou hors ligne, l'identité numérique fonctionne comme une extension des documents d'identité physiques existants tels que les passeports, les permis de conduire et les cartes bancaires. À son niveau le plus simple, l'identité numérique est une manière de représenter avec précision et en toute sécurité qui vous êtes.

Liste non exhaustive des cas d'utilisation de l'identité numérique :

- La production d'un certificat de naissance ou d'un permis de conduire
- L'intégration d'une personne dans un service numérique
- Vérification de l'âge en ligne, notamment dans la protection des mineurs en ligne
- La signature d'un contrat commercial
- L'ouverture d'un compte bancaire
- Remplir une déclaration d'impôts
- Une demande d'admission à l'université ou au collège
- Demander une ordonnance médicale
- Louer une voiture et prouver qu'on est capable de la conduire
- S'enregistrer dans un hôtel
- Vérification de l'identité

- Partager des données d'intérêt général pour un usage public
- Améliorer l'interaction politique et/ou le vote
- Embarquement dans un avion
- Passage d'une frontière

Bien plus qu'un simple certificat

Les moyens traditionnels d'identification servent à identifier leur titulaire et offrent une certaine sécurité, mais elles présentent des lacunes importantes. Les données associées aux documents d'identité actuels ne sont pas portables, sont fragmentées et échappent au contrôle du titulaire de la carte.

L'identité numérique va au-delà des fonctions d'authentification de base permises par les documents traditionnels attestant de l'identité des personnes ou des entreprises. Contrairement aux moyens traditionnels , qui, par nature, sont immuables et limités dans leurs contenus, un justificatif d'identité numérique permet l'ajout de nouvelles informations. Les différentes informations peuvent être "compartimentalisées" et utilisées avec différents niveaux de sécurité.

Un portefeuille numérique ou "digital wallet" héberge tous les documents d'identité et titres sécurisés digitalisés. Ce portefeuille peut être directement accessible depuis un smartphone. Outre son confort d'utilisation, le portefeuille numérique offre aux citoyens et aux entreprises un contrôle total sur leurs données personnelles, avec la liberté de décider quelles informations ils partagent, quand et avec qui ils souhaitent les partager.

Instaurer une confiance

En permettant le contrôle renforcé de l'utilisateur sur ses données et la transparence du processus, l'identité numérique peut contribuer à renforcer la confiance dans la société. Cela nécessite toutefois, une sensibilisation plus générale des utilisateurs à l'importance de la protection et la maîtrise de leurs données.

Les outils et les services d'identité numérique peuvent aider les gouvernements et les entreprises à instaurer de la confiance en s'engageant à proposer un service sécurisé et respectueux de la vie privée. Les organismes des secteurs public et privé peuvent démontrer leur engagement à responsabiliser et à protéger les utilisateurs en concevant des solutions et des services centrés sur l'humain. Si la technologie offre de nombreuses opportunités, elle ne peut pas à elle seule, résoudre tous les problèmes liés au manque de confiance.

Contribuer à l'intérêt général

Plusieurs études ont révélé que la population était en faveur de la promotion de l'identité numérique. Par exemple, une récente enquête du CCIAN a révélé que 78 % des canadiens estiment qu'il est très important ou assez important que le gouvernement canadien agisse rapidement pour développer une identité numérique sûre et sécurisée pour l'ensemble du pays. Et 2/3 des canadiens affirment que la pandémie a renforcé l'importance de disposer d'une identité numérique sûre, fiable

et respectueuse de la vie privée pour faciliter les transactions en ligne en toute sécurité. Le sondage a également révélé qu'une forte majorité des canadiens sont d'accord pour dire qu'ils devraient avoir accès aux données personnelles recueillies à leur sujet par les gouvernements et les entreprises privées.

De même, l'enquête Eurobaromètre a révélé que 72 % des européens souhaitent savoir comment leurs données sont traitées lorsqu'ils utilisent les réseaux sociaux. 63% des citoyens de l'UE souhaitent une identité numérique unique sécurisée pour tous les services en ligne.

À l'échelle mondiale, l'étude IPSOS MORI d'EY 2021 indique que les citoyens sont largement favorables à des services publics plus numériques, s'ils permettent de renforcer le contrôle de l'utilisateur. En revanche, en fonction des pays et des cultures, tous ne perçoivent pas le concept d'identité numérique de la même manière.

Les avantages de ces nouveaux systèmes numériques ne sont toutefois pas garantis, et les décideurs et les gouvernements se heurtent à de nombreux obstacles immédiats et persistants.

Il est urgent d'agir !

Il est recommandé que les responsables politiques explorent les projets pilotes relatifs à l'identité numérique et les projets internationaux en cours. Acquérir cette expérience pratique facilite la compréhension des opportunités liées à l'identité numérique.

L'absence de positionnement d'un gouvernement sur le sujet aurait des conséquences importantes. Un des risques majeurs serait notamment de perdre un positionnement stratégique à l'échelle mondiale, en laissant la priorité aux gouvernements et aux organismes privés qui se sont saisis du sujet. Le manque de coordination entre les acteurs publics et privés pourrait aussi soulever de graves questions de souveraineté et aggraver les attaques de cybersécurité.

Au-delà du déploiement, pour être une réussite, la technologie doit être socialement acceptée et adoptée. Pour se faire, l'identité numérique doit reposer sur un cadre de confiance qui justifie auprès des utilisateurs - citoyens, consommateurs, entreprises - que les acteurs en charge assurent leur devoir de diligence. Des justificatifs d'identité bien conçus peuvent permettre aux individus de bénéficier d'une plus grande confidentialité et d'un meilleur contrôle de la protection et du partage de leurs données. Les organismes qui adoptent et mettent en œuvre les meilleures pratiques pour assurer le devoir de diligence contribuent de facto à atténuer les risques encourus. Ce qui peut également les protéger de certaines responsabilités.

Un écosystème d'outils et de services d'identité numérique solide et sécurisé, fondé sur des principes universels, peut rapidement faire progresser le paysage des priorités civiques et sociales. Par exemple, l'identité numérique peut soutenir l'engagement démocratique, civique et social en connectant les gouvernements aux citoyens, notamment lors d'un besoin d'assistance ou d'une réponse à renseignement rapide. Cet écosystème peut également favoriser le partage de données pour l'intérêt général ou l'engagement civique local. Concrètement, cela peut se traduire par un partage de données médicales pour aider à identifier les traitements et les remèdes à des problèmes médicaux.

https://diacc.ca/2022/06/02/diacc-2022-industry-survey-report/
https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_en
https://www.ey.com/en_ca/government-public-sector/how-can-digital-government-connect-citizens-without-leaving-the-disconnected-behind

Un modèle unique ne fonctionnera pas pour tous

L'un des enseignements de ces dernières années, est que les individus ont des opinions très différentes sur la place que la technologie devrait avoir dans notre quotidien.

Cette réflexion rejoint la question de la confiance envers les institutions et les acteurs privés qui développent des technologies. Pour que l'identité numérique soit un succès, cette confiance doit être gagnée. Selon le contexte et les croyances de chacun, les facteurs qui permettront d'établir une relation de confiance avec une solution technologique varieront considérablement.

Pour évaluer l'impact que les recommandations auront sur différents groupes de la société, ce rapport fait appel à une étude mondiale EY/ IPSOS MORI de 2021 intitulée "Comment un gouvernement numérique peut-il connecter les citoyens sans oublier personne ?" .

Sur un panel de sept groupes de personnes, quatre groupes de personnes ont été sélectionnés pour mettre en lumière les recommandations du rapport - "Capable Achievers", "Struggling Providers", "Privacy Defenders", and "Tech Skeptics" - représentent des segments importants de la population. Chaque groupe ainsi que leurs besoins et problèmes numériques seront examinés ci dessous.

Catherine est une "Capable Achievers: ***Indépendants, accomplis et satisfaits de leur vie, ce sont des technophiles pragmatiques qui s'adaptent à l'innovation numérique. Ils sont convaincus que les gouvernements utilisent leurs données de façon appropriée, mais se préoccupent du fait qu'elles peuvent tomber entre de mauvaises mains.***

Catherine a 54 ans. Elle vit avec son mari dans leur maison en banlieue. Avec deux enfants à l'université, elle jouit d'une vie confortable, grâce à son emploi de cadre dans une entreprise mondiale de médias. Catherine se sent satisfaite et est optimiste quant à son avenir. Elle possède et utilise quotidiennement un smartphone et un ordinateur portable pour travailler, rester en contact avec ses amis et sa famille, suivre l'actualité, regarder ses émissions préférées en streaming, faire des achats en ligne et gérer ses finances. Elle considère la technologie comme une force positive qui facilite les tâches. Mais elle n'a pas encore acheté d'appareils connectés. Catherine privilégie la rapidité et la facilité lorsqu'elle interagit avec les services publics - ce qu'elle fait principalement pour les tâches administratives et concernant la santé. Elle n'aime pas devoir communiquer ses données personnelles à chaque fois qu'elle accède à un site Web gouvernemental et préférerait disposer d'un portail unique et d'une identité numérique unique de citoyen.

Jonathan est un Struggling Providers: *Il s'agit de jeunes ayant tendance à occuper des emplois mal rémunérés et moins sûrs. Ils ont recours plus que la moyenne à l'aide sociale. Ils sont ambivalents à l'égard de la technologie, n'y ont pas accès ou ne possèdent pas les compétences pour que celle-ci améliore considérablement leur qualité de vie.*

Âgé de 34 ans, Jonathan, qui a une femme et deux filles, vit en ville où il travaille dans une entreprise de messagerie. Il a un problème de santé qui limite sa capacité à effectuer différents types de tâches. Sa femme reste à la maison pour s'occuper des enfants et de son père âgé, qui vit avec eux. La famille dépend du revenu de Jonathan. Comme il n'a pas d'indemnités de maladie, de pension ou d'autres avantages sociaux et qu'il n'a aucune garantie d'emploi régulier, il est inquiet pour l'avenir. La famille compte sur les services publics, mais Jonathan pense que le gouvernement comprend mal la situation de sa famille et que le soutien qu'il reçoit n'est pas suffisant. Jonathan manque de confiance et de compétences pour utiliser la technologie. Il possède un smartphone à carte et un ordinateur portable reconditionné, mais ne peut pas s'offrir l'internet haut débit. Il ne croit guère que la technologie moderne puisse améliorer la vie. Il préfère interagir avec le gouvernement ou les fournisseurs de services publics par téléphone ou par courriel plutôt que par l'intermédiaire d'un site Web - bien qu'il soit ouvert à l'utilisation des réseaux sociaux. Il apprécierait un portail gouvernemental unique permettant d'accéder à tous les services - si seulement il pouvait s'y connecter. Il est assez ambivalent quant au fait que le gouvernement partage ses données personnelles, que ce soit en interne ou avec des entreprises privées.

David est un "Privacy Defenders": *Ils ont tendance à être plus âgés, indépendants et à l'aise financièrement. Ils accordent de l'importance à la technologie et aux avantages qu'elle leur procure, mais sont extrêmement prudents pour ce qui est de partager leurs données personnelles avec le gouvernement ou des entreprises privées.*

David a 48 ans, vit avec sa femme et était heureux de sa vie avant la pandémie, mais il est désormais conscient de la nécessité de maintenir ses compétences à jour au cas où il aurait besoin d'un nouvel emploi. Lorsque David interagit avec les services gouvernementaux, il est rarement satisfait. Il est frustré par l'inefficacité de l'accès aux services et souhaiterait de meilleures interactions, plus rapides et plus faciles, ainsi qu'un personnel plus compétent qui le traite avec respect. David a une conscience aiguë de son empreinte numérique et est prudent lorsqu'il partage ses données personnelles. La vie privée et l'anonymat sont des priorités essentielles pour lui. Il se méfie des réseaux sociaux et partage un minimum d'informations personnelles sur ces sites. Bien qu'il souhaite que les services soient davantage personnalisés pour répondre à ses besoins individuels, il limite la quantité de données qu'il partage avec les agences gouvernementales et les entreprises privées. David est mal à l'aise à l'idée que le gouvernement partage ses données à l'intérieur ou à l'extérieur du secteur public, même si cela peut aider à la planification et à la prise de décisions qui profiteraient directement aux citoyens. Bien qu'il s'impatiente de devoir répéter ses données personnelles lorsqu'il interagit avec les agences gouvernementales, il préfère encore cela à la possession d'un identifiant numérique de citoyen qui permettrait à

https://www.ey.com/en_ca/government-public-sector/how-can-digital-government-connect-citizens-without-leaving-the-disconnected-behind

différentes organisations d'accéder à ses données personnelles. Tant qu'il ne sera pas rassuré sur la sécurité totale de ses données, il ne souhaite pas voir de solutions numériques avancées dans les services publics.

Christine est une "Tech Skeptics": ***Plus âgés, touchant un revenu plus faible et relativement insatisfaits de leur vie, ils ne font pas confiance au gouvernement et sont sceptiques quant aux avantages que leur procure la technologie. Ils ont tendance à s'opposer au partage de données, même si l'objectif est clair.***

Christine est veuve et a des enfants adultes. Elle va bientôt quitter son emploi au service des ressources humaines d'une entreprise de logistique. Elle est préoccupée par sa sécurité financière : ses plans de retraite ont été endommagés par la crise financière il y a plus de dix ans et ne sont toujours pas rétablis. Elle est sceptique quant aux avantages de la technologie, qu'elle considère comme profitant aux riches et aux puissants, plutôt qu'aux citoyens ordinaires. Malgré cela, elle possède un smartphone, un ordinateur portable et un téléviseur, qu'elle utilise pour des tâches limitées, comme rester en contact avec ses amis et sa famille et faire des achats. Elle ne voit pas l'intérêt d'améliorer ses compétences numériques et n'est pas convaincue que l'innovation technologique est essentielle pour relever les défis économiques et sociaux auxquels le monde est confronté. Bien que Christine souhaite que l'accès aux services soit plus facile, elle est opposée à la création d'un identifiant numérique unique du citoyen, surtout si celui-ci est lié à des données personnelles relatives aux revenus. Elle s'oppose fermement à ce que le gouvernement partage ses données personnelles - que ce soit en interne ou avec des entreprises privées - même lorsqu'il y a un objectif clair, comme la lutte contre les activités criminelles ou le terrorisme. Elle pense que les avantages éventuels du partage des données seraient annulés par la menace qui pèserait sur sa vie privée et sa sécurité. Elle se méfie également du partage des informations personnelles avec les entreprises lorsqu'elle effectue des transactions.

Lors de la conception d'une politique, il faut comprendre que tout le monde ne perçoit pas l'identité numérique de la même manière. C'est pourquoi le fait de travailler avec différents personnages tels que Catherine, David, Christine et Jonathan peut aider à identifier les points communs et les différences pour instaurer la confiance. Cela aide à définir les principes fondamentaux qui permettent de répondre à leurs préoccupations.

Les avantages et les risques du déploiement de l'identité numérique

Gérer les risques pour optimiser les avantages

Pouvoir s'appuyer sur un écosystème qui protège les données et offre aux utilisateurs un accès aux services publiques et privées plus efficace est inestimable.

Pour les innombrables petites et moyennes entreprises du monde entier, les économies réalisées en matière d'approvisionnement, d'accès aux services financiers, et autres opérations grâce à un système d'identité numérique pourraient représenter plusieurs milliards de dollars de valeur et d'investissements par an. De même, dans le secteur financier mondial, les gains d'efficacité opérationnelle créés par la réduction des coûts de traitement manuel et la limitation de la fraude apporteraient des avantages substantiels aux consommateurs et aux entreprises.

Cette innovation peut également donner aux citoyens le pouvoir d'accéder à leurs propres données, les gérer et les partager. L'utilisateur pourra avoir le contrôle de toutes les informations importantes dont il a besoin, sur sa vie privée ou professionnelle.

Comme pour toute nouvelle technologie, il existe des risques associés à la mise en application des politiques d'identité numérique et ils ne sont pas négligeables.

Cependant, comme le présent rapport espère le démontrer, une mise en œuvre bien conçue et correctement gouvernée de l'identité numérique peut servir à amplifier les avantages et à atténuer les risques.

Interopérabilité et efficacité

Lorsqu'une personne présente un justificatif d'identité traditionnel , les données contenues dans ce dernier sont statiques. Elles ne peuvent pas circuler automatiquement vers ou depuis l'entité qui les vérifie. Elles ne peuvent pas remplir automatiquement des formulaires ou faire l'objet d'une vérification automatique de l'authenticité.

Au contraire, l'identité numérique, facilite toutes ces caractéristiques. Par exemple, l'identité numérique peut être utilisée dans le cadre des services de santé pour faciliter le transfert des dossiers médicaux d'un hôpital au médecin d'un patient. Ou encore, grâce à l'identité numérique, un individu peut remplir automatiquement les champs d'un formulaire, déverrouiller l'accès à des informations précédemment soumises ou valider des informations d'identification externes.

CATHERINE

J'ai utilisé mon identité numérique pour signer un nouveau contrat de fournisseur - cela a non seulement prouvé que j'étais un membre légitime de notre association professionnelle.

Minimisation des données

Lorsqu'ils utilisent des moyens d'identification traditionnels, les personnes partagent souvent plus d'informations que nécessaire. A contrario, les justificatifs d'identité numériques permettent aux personnes de ne partager que les informations proportionnellement nécessaires au contexte spécifique. Le fait de "compartimentaliser" les données d'identité permet (si on le souhaite) de préserver l'anonymat d'une personne.

Une illustration de ce principe se traduit lors de la mise en œuvre concrète de la protection des mineurs en ligne. En effet, une protection efficace des mineurs en ligne nécessite leur identification et l'encadrement de l'accès aux services et contenus en ligne. La minimisation des données consiste à donner à chacun la possibilité de ne délivrer que la preuve d'un seul attribut (preuve de majorité, preuve de résidence, preuve de diplôme, etc.) sans révéler les autres éléments qui constituent une identité. La minimisation des données apporte une réponse pour identifier l'âge des utilisateurs tout en préservant leur vie privée.

DAVID

J'ai été heureux d'apprendre que si l'identité de mon enfant est contrôlée pour acheter de l'alcool, il est en mesure de prouver qu'il a l'âge légal de boire grâce à un justificatif d'identité numérique. Au lieu d'utiliser une pièce d'identité sur laquelle figurent son nom, son adresse, sa date de naissance et d'autres informations personnelles, il ne pourra prouver que son âge

Flexibilité

Contrairement à une carte d'identité traditionnelle, un portefeuille numérique permet à une personne de gérer les informations qui y figure et d'ajouter (ou de supprimer) les justificatifs numériques associés.

Par exemple, au fur et à mesure de ses études universitaires, une personne peut choisir d'associer à son identité numérique une série de nouveaux justificatifs qu'elle pourra ensuite choisir d'utiliser dans divers contextes tels que "âge de voter, droit de vote", "âge de la majorité, droit d'acheter de l'alcool", "étudiant à temps plein, droit à l'emploi".

Le fait que ces informations d'identification puissent être pertinentes pour divers services et qu'elles puissent être plus ou moins sensibles explique pourquoi elles doivent être compartimentées et soumises à divers niveaux de sécurité.

Inclusion

Étude de cas : Le système Aadhaar en Inde

Pour plus d'un milliard d'individus dans le monde, l'absence de moyen de prouver son identité empêche l'accès aux biens et services de base, selon l'étude des Nations unies intitulée "Plan d'action du secrétaire général pour la coopération numérique". Selon cette étude, "une 'bonne' identité numérique, qui préserve la vie privée des gens et leur permet de contrôler leurs informations, peut leur donner les moyens d'accéder à des services dont ils ont grand besoin". Des initiatives telles que "Identification for Development" et le groupe de travail des Nations unies sur l'identité légale peuvent aider les pays à réaliser le potentiel de transformation des systèmes d'identification numérique.

L'Inde a créé le plus grand système d'identité biométrique au monde, utilisant des empreintes faciales, un scan du visage et des yeux. Aadhaar, qui signifie "fondation", a été mis en place en 2009 comme application centralisée pour permettre à chaque résident du pays d'établir facilement son identité. À la fin de 2021, l'Unique Identification Authority of India a indiqué que 1,3 milliard de personnes, soit environ 99 % des adultes indiens, s'étaient inscrites à Aadhaar.

Le programme a amélioré l'inclusion financière en ouvrant l'accès aux comptes bancaires et la prestation de services en facilitant le transfert des fonds de soutien du gouvernement aux bénéficiaires. Le programme est crédité d'avoir fourni une infrastructure clé pour la distribution alimentaire et financière qui a contribué à maintenir l'extrême pauvreté à des niveaux pré-pandémiques pendant le COVID-19. Le "Rapport sur l'état d'Aadhaar" de 2019 en Inde, qui a interrogé 167 000 utilisateurs, a révélé que 92 % des personnes interrogées étaient satisfaites du fonctionnement du système . Ces résultats sont une indication du pouvoir que l'identité numérique peut avoir lorsqu'elle est exploitée pour le bien social.

Engagement démocratique et social

Étude de cas : Le système de vote électronique de l'Estonie

L'Estonie utilise l'identification numérique pour permettre le vote en ligne depuis 2005. Près de la moitié des électeurs estoniens ont utilisé le "I-voting" pour voter lors des dernières élections du Parlement européen en 2019. À la suite de la pandémie de COVID-19, le système estonien s'est avéré être non seulement pratique, mais aussi un outil précieux pour soutenir les mesures de santé publique.

https://stateofaadhaar.in/download-reports.php

Facilitation du partage des données pour l'intérêt général

Case Study: Barcelona's Salus.Coop

La Human Technology Foundation a exploré le concept de "data altruisme", ou partage des données pour l'intérêt général . Selon le Data Governance Act , qui a été adopté en mai 2022, l'altruisme des données est "le partage volontaire de données basé sur le consentement ou les permissions à des fins d'intérêt général telles que les soins de santé, la lutte contre le changement climatique ou l'amélioration des services publics". Ce système innovant se distingue des deux principaux systèmes de partage de données existants : le système commercial (dans lequel les données sont traitées sur un marché concurrentiel) et le système d'open data (dans lequel certains types de partage de données sont rendus obligatoires par la loi). L'innovation de l'altruisme des données est rendue possible par la création d'organisations altruistes, qui doivent être perçus comme des des tiers de confiance, indépendants et sans but lucratif, garantissant la transparence totale de la collecte et du partage des données à des fins d'intérêt public. Un exemple probant est le travail effectué par Javier Creus, qui a créé "Salus.Coop" à Barcelone, une coopérative de données citoyennes à but non lucratif pour la recherche sur la santé qui facilite le partage par les utilisateurs de leurs données de santé à des fins de recherche médicale.

Des développements d'une telle ampleur au service de l'intérêt public ne sont possibles que par le traitement massif des données de santé. L'identité numérique pourrait contribuer à initier un mouvement social qui fait du partage des données pour le bien public une norme sociale.

https://www.human-technology-foundation.org/news/data-altruism-report-seen-by-grimaud-valat
https://www.consilium.europa.eu/en/press/press-releases/2022/05/16/le-conseil-approuve-l-acte-sur-la-gouvernance-des-donnees/

Surveillance et absence de responsabilité

Dans de nombreux pays, l'opinion publique est très préoccupée par l'impact et les risques potentiels des systèmes d'identité numérique. Les craintes se sont accrues dans le contexte où la pandémie de COVID-19 a accéléré l'expansion des usages numériques. Le risque d'abus des gouvernements à utiliser l'identité numérique à des fins de surveillance est généralement en tête de liste des préoccupations.

Ces craintes ne sont pas seulement théoriques. En 2017, par exemple, un rapport du Center for Internet and Society a analysé les données associées à Aadhaar. Il a été constaté que 100 à 135 millions de numéros d'identification Aadhaar et 100 millions de numéros de comptes bancaires avaient été divulgués.

CHRISTINE

En théorie, j'aimerais que les services publics soient plus faciles d'accès, et je veux absolument minimiser les dépenses gouvernementales en matière de bureaucratie inefficace, mais je suis très sceptique. Que se passe-t-il s'ils peuvent consulter mes coordonnées et mes propres informations privées si je commence à utiliser l'identification numérique ?

Cybersécurité

De grandes bases de données contenant d'immenses quantités d'informations personnelles sont des cibles attrayantes pour les cyberattaques, ce qui constitue une menace de plus en plus pressante pour les gouvernements et les organisations du secteur privé.

Dans l'exemple d'Aadhaar en Inde, le système a été entaché de lacunes attribuées à des problèmes de conception du projet et à l'incapacité de respecter l'obligation de sécurité. L'absence de tels contrôles a conduit à une fuite de données en 2018 qui a rendu publiques des données Aadhaar sur 200 sites gouvernementaux officiels. Le problème était si répandu qu'une simple recherche sur Google révélait des milliers de bases de données ainsi que des données démographiques, notamment des numéros Aadhaar, des noms, des noms de parents, des numéros de compte personnel (PAN), des numéros de téléphone mobile, la religion, les marques, le statut de rejet des demandes, les numéros de compte bancaire, les codes IFSC et d'autres informations.

Coût, complexité et collaboration

Étude de cas : Le cadre de confiance pour l'identité numérique de l'Australie (TDIF)

Depuis 2015, l'Australie poursuit un programme d'identité numérique à l'échelle de l'ensemble du gouvernement, guidé par les exigences énoncées dans les orientations du gouvernement intitulées : Trusted Digital Identity Framework (TDIF). Le programme vise à fournir une vérification d'identité à travers une gamme de services gouvernementaux et d'offres du secteur privé.

Le secteur financier australien va de l'avant avec des développements dans le cadre actuel du TDIF. Quatre grandes banques australiennes vont coopérer avec Australian Payments Plus pour développer son initiative d'identité numérique, ConnectID. Les banques joueront le rôle de fournisseurs d'identité dans une série d'essais. ConnectID, a été accrédité l'année dernière pour réaliser un échange d'identité numérique dans le cadre du TDIF.

Tout au long de l'année 2021-22, le TDIF a approuvé plusieurs fournisseurs d'identité numérique, dont Mastercard, Australia Post, le bureau des impôts australien et d'autres. Ce programme répond à certains besoins et préoccupations du public liés à la gestion des pandémies.

Les leçons tirées de l'exemple australien ? Se concentrer sur les besoins des secteurs public et privé, en plaçant les avantages et la sécurité des personnes au centre de la conception, est une combinaison gagnante. Toutefois, pour progresser, il faut des investissements importants et durables.

Comprendre la technologie et la terminologie de l'identité numérique

L'évolution de l'identité numérique

L'identité numérique a évolué rapidement et continue d'évoluer à mesure que l'expérience utilisateur, la sécurité, la confidentialité et la gestion des consentements prennent le devant de la scène. Si les modèles de gouvernances discutées au départ visaient plutôt une approche cloisonnée et centralisée, l'ère du temps semble à présent valoriser des modèles plus fédérés, décentralisés et hybrides.

https://www.dta.gov.au/our-projects/digital-identity/trusted-digital-identity-framework

CENTRALISÉE :
Une seule organisation stocke les données relatives à l'identité numérique de ses utilisateurs.

FÉDÉRÉE :
Une seule institution est chargée d'établir et de maintenir l'identité à travers plusieurs entreprises. Celle-ci est moins fragmentée à travers un écosystème numérique donné.

DÉCENTRALISÉE :
Il s'agit d'un modèle plus "distribué" dans lequel l'utilisateur contrôle sa propre identité. A l'image du bitcoin, aucune institution centralisée ne la "détient". Dans ce scénario, l'identité numérique est autonome, indépendante et transférable à travers de nombreuses organisations.

Les dernières tendances

Réseaux d'identité numérique autonomes

Le modèle le plus récent d'identité numérique - l'identité décentralisée - avec ses concepts transférables d'"identité auto-souveraine", est conçu pour que le contrôle de la vie numérique soit fermement entre les mains des individus. Il s'agit d'un changement de paradigme dans la façon dont nous voyons l'identité numérique, offrant aux utilisateurs la promesse d'une meilleure sécurité et d'une plus grande confidentialité grâce au contrôle de l'empreinte numérique d'une identité donnée. Elle promeut le potentiel d'un écosystème connecté dans lequel l'inscription à une identité numérique unique et portable suffit pour accéder aux services numériques de manière sûre et transparente.

De plus en plus de programmes nationaux d'identité numérique de cette nature sont lancés par des pays de toutes les régions du monde (Belgique, Norvège, Inde, Japon, Thaïlande, Turquie), qui s'engagent dans l'adoption de l'identité numérique dans la vie quotidienne des citoyens.

Une expérience utilisateur sûre et fluide dans les secteurs public comme privé.

L'expérience du client final avec une sécurité renforcée à travers les différents canaux est devenue une partie intégrante de l'établissement de la confiance numérique. Par exemple, l'alliance Fast IDentity Online (FIDO) a développé des normes d'authentification basées sur la cryptographie à clé publique, qui est plus sûre que les mots de passe et les codes à usage unique par SMS.

Les utilisateurs d'identité numérique seraient ainsi en mesure de transmettre une seule fois et en toute sécurité, des informations les concernant à un gouvernement ou à une entreprise. A partir de là, ils pourront confirmer quand et comment ces informations peuvent être utilisées pour différents services. En transmettant "une seule fois les données",

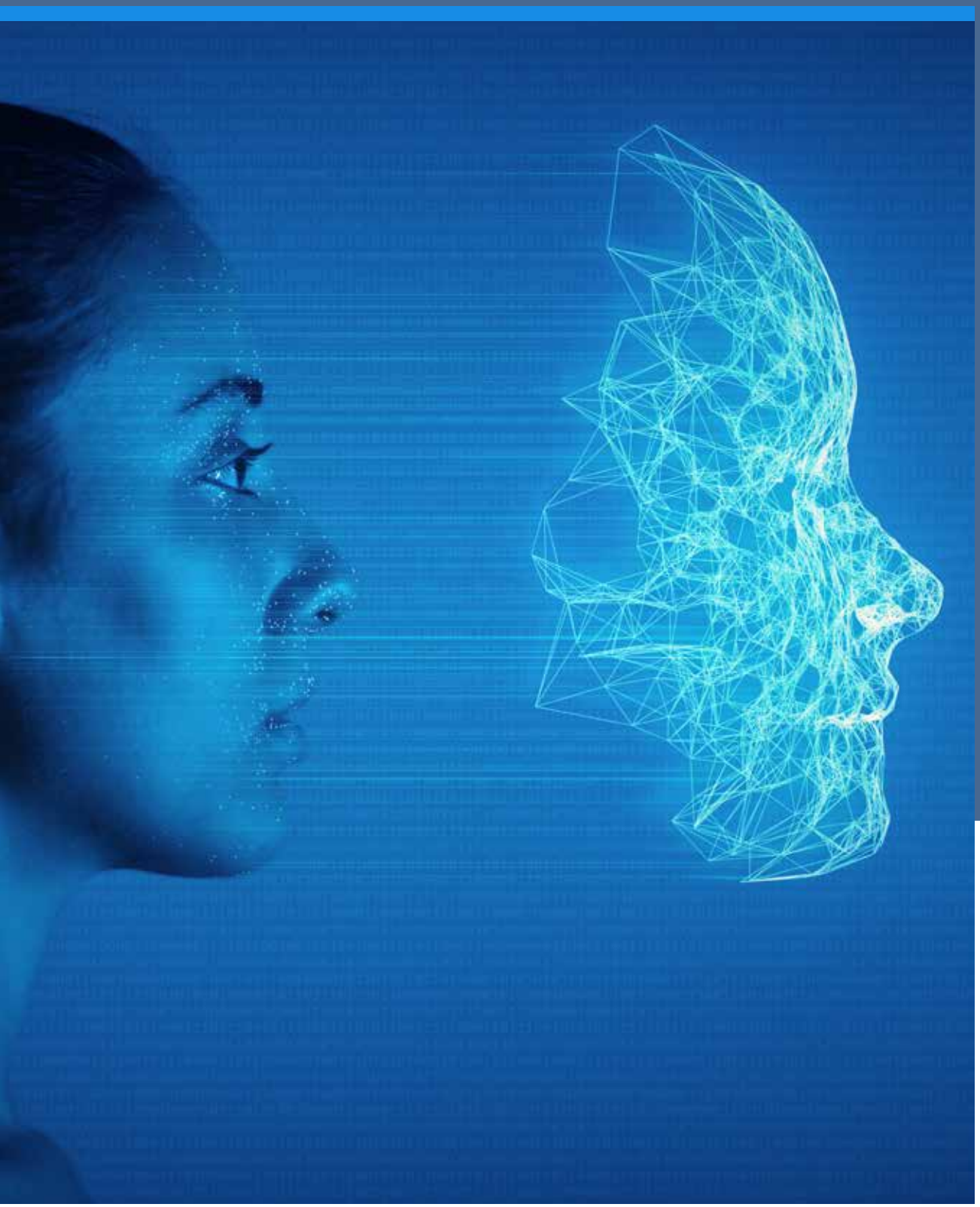
l'utilisateur sera libéré de la nécessité de gérer des dizaines de mots de passe, sans jamais garantir la transmission entre les différents services d'une même organisation. L'identité numérique et l'interopérabilité des services facilitent l'accès aux services des secteurs public et privé qui prenaient auparavant beaucoup de temps, tout en étant plus sûrs.

Ces normes et approches améliorées signifient que les utilisateurs peuvent créer et vérifier leur identité dans le secteur privé, puis réutiliser cette identité dans le secteur public. De même, les utilisateurs peuvent créer une identité en utilisant un service public et en propager l'utilisation dans les secteurs public et privé.

Une standardisation en cours

L'interopérabilité et la compatibilité sont essentielles à l'adoption et à la réalisation du potentiel des programmes d'identité numérique, et l'émergence de nouvelles normes est un facteur clé. Par exemple, la réglementation européenne sur l'identification électronique et la confiance (eIDAS) a rendu obligatoire l'interopérabilité des identités numériques dans les échanges électroniques. La Commission européenne a recommandé la création d'un portefeuille d'identification universel utilisable dans toute l'Europe d'ici 2030. Au niveau international, l'évolution des normes se poursuit, par exemple :

- L'Organisation de l'aviation civile internationale travaille actuellement sur la structure de données logiques version 2 (LDS2). Il s'agit de la prochaine évolution du passeport électronique.
- Le comité technique 14 SC17 WG10 de l'Organisation internationale de normalisation (ISO) a commencé à travailler sur des normes de vérification pour les permis de conduire mobiles.
- "Travel Pass" est disponible auprès du groupe de travail sur l'identité mobile de l'IATA.
- Il existe d'autres exemples tels que "ISO/IEC 18013", "FIDO2", "NIST SP 800-63-3" et "OIDC Bridges", entre autres. Les acronymes peuvent être quelque peu impénétrables, mais toutes ces normes en progrès contribuent à jeter les bases d'une identité interopérable, compatible, voire transfrontalière, dans un souci de sécurité et de fiabilité



Recommandations pour la conception de la politique

1: Les utilisateurs doivent être au coeur de la politique d'identité numérique

"Prioriser les droits et les besoins des individus"

La politique d'identité numérique doit être conçue à partir des besoins de l'utilisateur, et plaçant les individus au centre du processus. Une grande force de l'identité numérique est qu'elle est flexible. Ses nombreuses fonctions peuvent être utilisées de différentes manières, permettant de toujours s'adapter au besoin de l'utilisateur.

Les fonctions de l'identité numérique inversent la situation actuelle dans laquelle les gens doivent concevoir leur comportement en fonction des services. A présent, ce sont les services qui sont conçus autour de la personne.

* L'identité numérique se doit d'être INCLUSIVE

"Facilement accessible à tous ceux qui souhaitent l'utiliser".

Il est essentiel que l'identité numérique soit inclusive, équitable et accessible à tous ceux qui souhaitent l'utiliser si l'on veut que son plein potentiel soit réalisé à l'échelle internationale dans les années à venir.

L'élaboration d'une politique d'identité numérique doit tenir compte de la fracture numérique. Les besoins des différents publics doivent être identifiés afin de proposer des alternatives et un soutien à long terme. L'accès aux services numériques est plus difficile pour certains groupes, notamment en matière d'infrastructures et de compétences. Les obstacles peuvent prendre de nombreuses formes, notamment économiques/financières, éducatives, sociales, médicales et de santé mentale. La politique devrait guider les services pour qu'ils soient conçus de manière à ce que toutes les personnes légitimes puissent y avoir accès.

> *J'aimerais utiliser davantage de services numériques, mais mon beau-père et moi souffrons tous deux de problèmes de santé, ce qui rend plus difficile l'utilisation de la technologie, et nous avons également un budget très serré - nous ne pouvons pas nous le permettre si cela doit coûter plus cher.*
>
> **– JONATHAN**

https://decidim.org/
https://www.linkedin.com/company/imagia-cybernetics/

L'adoption de l'identité numérique doit être un acte VOLONTAIRE

"Il ne s'agit pas d'une obligation, et des services alternatifs seront toujours disponibles"

Alors que les gouvernements exigent des justificatifs d'identité faisant autorité sur le plan juridique, les nouvelles politiques doivent permettre aux gens d'avoir la possibilité de choisir d'utiliser les nouveaux justificatifs numériques, tout en préservant la possibilité d'utiliser des justificatifs alternatifs.

> *Je vieillis. Tout cela ne m'intéresse plus. Mais, j'ai encore besoin de soutien dans mes démarches administratives".*
>
> ***– CHRISTINE***

L'identité numérique doit être ROBUSTE

"Toujours disponible en cas de besoin, partout et à tout moment "

Les services d'identité doivent être suffisamment robustes et fiables pour permettre l'accès aux ressources qu'ils procurent en continu. Il s'agit notamment de s'assurer que le service et les entrées du service soient disponibles lorsqu'ils doivent l'être et d'éviter les points de défaillance uniques. La politique et l'architecture des services associés détermineront la manière dont ces services seront utilisés. Il faut notamment veiller à ce que l'accès ne puisse être refusé à un utilisateur du réseau sans raison légitime.

> *Je suis en déplacement dans le monde entier pour mon travail, et je dois rester connectée 24 heures sur 24 et 7 jours sur 7. J'attends absolument d'accéder à ce dont j'ai besoin quand j'en ai besoin.*
>
> ***– CATHERINE***

La politique d'identité numérique doit être intuitive, tant pour les institutions que pour les INDIVIDUS.

"Simple d'utilisation"

En pratique, les services d'identité devraient offrir aux utilisateurs des expériences familières, intuitives, simples et informatives, afin qu'ils puissent faire de bons choix. Ils devraient également respecter les normes industrielles modernes en matière d'accessibilité pour tous les citoyens et être disponibles pour tous les citoyens, quelle que soit leur capacité financière.

Par exemple, grâce à la mise en œuvre du principe "dites-le nous une fois", une personne peut être libérée de l'obligation de gérer des dizaines de mots de passe, sans jamais savoir si l'un de ses services a été compromis.

Les avantages offerts par l'identité numérique permettent de faciliter des processus d'accès aux services des secteurs public et privé qui prenaient auparavant beaucoup de temps, tout en étant plus sûrs.

> *Je deviens vraiment impatient avec les services qui me font perdre mon temps - j'ai été surpris de voir à quel point il était clair, simple et facile d'utiliser ce justificatif d'identité numérique. Mes questions et mes préoccupations concernant la confidentialité et la sécurité ont été clairement formulées et traitées*
>
> ***– DAVID***

La vie privée doit être au cœur de la politique d'identité numérique

"Le droit d'être laissé tranquille."

Les services de l'identité numérique ajoutent une nouvelle dimension au principe de la vie privée : la minimisation des données. Cela signifie qu'il ne faut pas recueillir auprès d'autrui plus d'informations que celles qui sont nécessaires au service. La minimisation des données permet de préserver l'anonymat d'une personne (si elle le souhaite).

Cette politique doit amener les solutions à offrir aux utilisateurs un contrôle de leurs données, ainsi qu'une garantie de confidentialité et de diligence.

Les politiques devraient guider les services afin de garantir qu'une personne puisse utiliser ses informations d'identité numérique sans surveillance, suivi, collusion ou traçabilité. L'exception étant les cas où la traçabilité est exigée par la loi, strictement nécessaire sans autre option, dans le respect des droits fondamentaux et dans le cadre de l'enquête du pouvoir juridictionnel applicable.

> *Je veux m'assurer que seul le minimum d'informations sur ma vie soit partagé lorsque je paie mes impôts, ou que j'achète du vin, ou que je vais à la banque. J'ai besoin de savoir qu'il existe des garanties pour protéger ma vie privée.*
>
> ***– CHRISTINE***

2: L'identité numérique doit renforcer le pouvoir des utilisateurs

"Les individus ont la possibilité d'accéder aux données concernant leur identité et de les utiliser pour leur usage personnel et pour l'intérêt général."

Une identité numérique offrant ce pouvoir aux entreprises, aux clients, et aux citoyens permettrait de renforcer la confiance dans les relations, d'élargir son utilisation, comme pour promouvoir la participation du public aux processus locaux, gouvernementaux et politiques.

Les politiques doivent être structurées de manière à guider le développement de services qui permettent aux individus d'effectuer des transactions en toute sécurité. Les services doivent notamment permettre de contrôler le flux d'informations.

Une politique qui permet et guide des services d'identité numérique bien conçus peut favoriser l'exercice des droits des citoyens et des résidents du monde entier, ainsi qu'améliorer leur participation publique.

Plus largement, des écosystèmes numériques réussis, construits autour de l'identité numérique, peuvent fournir des données précieuses aux gouvernements pour relever les défis socio-économiques, accroître la participation politique et permettre aux gens d'accéder aux biens et services dont ils ont besoin. Le travail effectué par Imagia au Québec, qui détecte et diagnostique le cancer grâce à des systèmes d'IA pilotés par des données d'imagerie médicale, en est un bon exemple. Des développements d'une telle ampleur qui servent l'intérêt public ne sont possibles que par le traitement en masse de données de santé de bonne qualité et interopérables.

L'identité numérique doit être contrôlée par l'utilisateur

"Les individus décident des données qu'ils veulent partager, avec qui, et dans quel but"

En pratique, la mise en œuvre de solutions d'identité numérique et de politiques directrices doivent donner aux personnes la possibilité de décider ce qu'elles veulent partager, avec qui et dans quel but, avec la possibilité de retirer leur consentement à tout moment.

> *Je veux m'assurer que mon identité reste MIENNE quoi que j'en fasse - je peux donc décider de ce qu'il advient de mes informations. Je peux changer d'avis si je ne veux plus qu'elles soient utilisées avec la certitude d'en avoir le contrôle total*
>
> ***– DAVID***

L'identité numérique doit être fondée sur le consentement éclairé

"Lorsque quelqu'un veut vérifier ou utiliser les données relatives à l'identité d'une personne, cette dernière choisit d'accepter ou non cette utilisation."

La politique d'identité numérique permet l'accès des utilisateurs aux informations relatives à leur identité et leur contrôle sur celles-ci, afin qu'ils puissent les partager lorsqu'ils s'inscrivent à un nouveau service ou lorsqu'ils accèdent à un service qu'ils utilisent déjà. Elle offre aux utilisateurs une visibilité et un contrôle sur la divulgation et le stockage de ces informations, en protégeant leur vie privée. C'est l'utilisateur qui décidera quelles informations divulguer, quand le faire, et à qui. Elle permet également la minimisation des données. Lorsque les informations partagées sont très sensibles, il est possible de renforcer la sécurité du consentement en ajoutant des étapes d'authentification supplémentaires.

Ce principe exige des précautions dans le contexte de la publicité numérique. Il est important que l'utilisation de l'identité numérique soit toujours fondée sur un consentement éclairé. Cela signifie que l'utilisateur doit disposer d'informations suffisantes pour prendre une décision éclairée sur la manière et le moment où son identité numérique est utilisée.

De même, les gouvernements et les organisations du secteur privé peuvent adapter les types de justificatifs numériques qu'ils peuvent demander aux individus de valider au moyen de l'identité numérique, généralement en fonction du niveau de risque des transactions concernées. Par exemple, diverses capacités et méthodes d'authentification peuvent être introduites selon les besoins, en fonction des risques, pour sécuriser une transaction. L'introduction d'une vérification "selon les besoins" en fonction du profil de risque de la transaction concernée renforce le contrôle personnel de son identité numérique.

> *J'ai demandé une carte de crédit l'autre jour et j'ai vérifié mon identité numériquement. J'ai donné mon consentement explicite pour qu'elle soit utilisée, et je n'ai eu besoin de partager que les éléments exacts d'information sur mon identité dont la banque avait besoin pour la transaction, et pas plus.*
>
> ***– CATHERINE***

* L'identité numérique doit permettre la portabilité des données

"L'utilisateur peut transférer les données relatives à son identité"

La politique d'identité numérique doit donner aux gens le pouvoir de contrôler le stockage et la transmission de leurs données. Les utilisateurs doivent avoir un accès et une possibilité de gestion simple de leurs données personnelles, et doivent être libres de les partager ou de les transférer sans contrainte excessive.

3: La politique d'identité numérique doit encourager la confiance par la gouvernance

"La responsabilité doit être claire"

La mise en place d'un écosystème d'identité numérique digne de confiance nécessite des accords de gouvernance des services afin de déterminer comment les services sont mis en œuvre et quels contrôles

sont mis en place pour garantir la sécurité des personnes et des données relatives à leur identité. En fin de compte, les services et les personnes devront se fier aux réglementations et aux contrats juridiques pour obtenir un niveau de certitude quant à la manière dont les personnes ou les entités sont protégées.

L'identité numérique doit être transparente

"Les politiques et les opérations sont accessibles et compréhensibles"

Les gens ont confiance dans les services lorsque le fonctionnement et la gouvernance du service sont transparents et compréhensibles. Les gens voudront avoir l'assurance que les données sensibles sont protégées. En particulier, ils auront besoin de savoir que les données personnelles sont traitées conformément aux lois sur la protection des données, y compris l'obtention du consentement explicite du sujet auquel ces données se rapportent, si nécessaire. Les personnes devront également comprendre, dans une certaine mesure, les processus utilisés pour établir, maintenir et sécuriser les identités numériques. Cela présentera un intérêt particulier pour les parties prenantes qui peuvent prendre des décisions commerciales sur la base des informations relatives à l'identité numérique qu'elles reçoivent.

> *ILorsque j'ai commencé à utiliser mon identité numérique, il était rassurant de comprendre simplement ce à quoi je m'engageais. Parfois, les "petits caractères" sont tellement déroutants et juridiques, mais cette fois, j'ai eu l'impression de connaître l'objectif et de comprendre les garanties mises en place*
>
> ***– JONATHAN***

La responsabilité de l'utilisation de l'identité numérique doit être bien définie

"La responsabilité de l'utilisation des données relatives à votre identité est toujours clairement établie."

La responsabilité consiste à s'assurer que toutes les parties agissent de manière responsable et respectent leurs obligations. Bien sûr, aucun système ni aucune organisation n'est parfait, et lorsque les choses tournent mal, les parties qui subissent une perte peuvent avoir droit à un recours.

> *Je veux être certain que si quelque chose se passe mal dans le cadre de l'utilisation de mon identité numérique, le responsable sera clairement identifié et j'aurais l'assurance de ne pas être lésé'.*
>
> ***– DAVID***

Les politiques d'identité numérique exigent de la sécurité

"Des contrôles réguliers et vigilants sont en place et évoluent pour assurer la sécurité des données relatives à l'identité"

Les systèmes d'identité numérique doivent garantir que les informations personnelles des personnes soient cryptées en toute sécurité, qu'elles ne soient partagées avec des prestataires de services choisis qu'avec le consentement de la personne concernée, et qu'elles soient protégées par des protocoles de sécurité stricts.

Les systèmes doivent être conçus de manière à éviter les points de défaillance uniques qui constitueront des cibles pour des pirates informatiques.

> *Je m'y connais assez en technologie pour savoir que les menaces de cybersécurité évoluent en permanence - j'ai besoin d'être sûre que mes données non seulement ne soient pas piratables maintenant, mais que l'écosystème est nécessaire pour garder mon identité sécurisée en permanence.*
>
> ***– CATHERINE***

L'identité numérique doit favoriser l'interopérabilité

"Les données relatives à l'identité sont transférables au sein d'un même système, mais aussi entre les services"

L'une des clés du développement d'un écosystème d'identité numérique réussi est l'interopérabilité, c'est-à-dire la capacité du système d'identité à échanger des données avec d'autres fournisseurs, systèmes, technologies et bases de données. Les gouvernements doivent s'efforcer d'élaborer une politique qui favorise l'interopérabilité entre les fournisseurs de services privés et publics à l'échelle nationale. Pour voir plus loin, il faudra également relever le défi d'assurer l'interopérabilité internationale des données et des technologies.

> *Puis-je utiliser mon identité numérique dans différents États ? La même identité numérique dans mon portefeuille numérique fonctionne-t-elle à ma banque, et chez mon courtier d'assurance automobile, et pour percevoir mes allocations ?*
>
> ***– JONATHAN***

Les normes industrielles, nationales et internationales jouent un rôle important dans le développement de l'interopérabilité.

La politique d'identité digitale devra résister à l'épreuve du temps, en se concentrant sur les résultats souhaités

"La politique est élaborée en se concentrant sur l'obtention de résultats mesurables."

Il convient de concevoir des politiques publiques qui resteront fidèles aux principes et au devoir de diligence décrits plus tôt, à mesure que les innovations technologiques et les normes sociétales évolueront. En pratique, il est utile de choisir des mots qui décrivent les résultats souhaités plutôt que des outils, méthodes ou technologies spécifiques.

La politique en matière d'identité numérique doit être développée afin de renforcer le dialogue public et privé

Compte tenu du contexte actuel de mésinformation et de désinformation autour du sujet de l'identité numérique, et afin de promouvoir sa compréhension tout en ajustant les politiques avant et pendant leur mise en œuvre, il est impératif de prendre en considération les retours de la population, notamment par exemple lors d'une consultation publique. La mise en œuvre de politique en matière d'identité numérique devrait impliquer un processus inclusif représentant de grands groupes de personnes issues de tous les milieux socio-économiques et géographiques.

Conclusion

L'expérience a montré que la réussite de cette transformation nécessite l'engagement des gouvernements et du secteur privé d' y associer des ressources. Ce rapport propose les principes clés pour développer un programme d'identité numérique soigneusement conçu intégrant les éléments nécessaires pour obtenir une large adhésion du public. Comme décrit précédemment, une conception réussie doit être centrée sur l'utilisateur, efficace et non coûteuse, avec des mesures adéquates en matière de confidentialité, de sécurité et de contrôle des utilisateurs. Le respect de ces critères de diligence et de sécurité est d'autant plus important à une époque où de nombreux citoyens s'inquiètent de l'ingérence des pouvoirs publics ou de la possibilité d'une utilisation abusive de leurs données.

Les auteurs de ce rapport notent que lorsque des politiques d'identité numérique sont conçues pour répondre aux critères de respect de la vie privée, d'inclusion et de soutien centré sur l'utilisateur, elles peuvent jouer un rôle majeur pour répondre aux préoccupations et aux besoins des utilisateurs, tant au niveau national qu'international. La conception de ces politiques doit veiller à ce que les besoins et les préoccupations des individus et des institutions soient pris en compte, en ce qui concerne la vie privée, l'utilisation de leurs données, l'interopérabilité et d'autres questions. Les gouvernements et les organisations pourraient ainsi réussir à mettre en place et à maintenir des services d'identité numérique acceptés et utilisés par le grand public, conditions nécessaires pour maximiser leurs avantages.

Annexe

Méthodologie de la conception de ce rapport

Ce rapport conjoint de HTF-CCIAN a été conçu grâce à un partenariat réunissant des contributeurs internationaux provenant de EY, McCarthy Tetrault et DTMV travaillant aux côtés d'un groupe d'intérêt spécial CCIAN composé de plusieurs représentants des secteurs privé et public, ainsi que d'un conseil consultatif présidé par le HTF, comprenant des experts internationaux en identité numérique, communication, politique et économie numérique.

Le conseil consultatif présidé par le HTF et le groupe d'intérêt spécial présidé par le CCIAN ont éclairé HTF et CCIAN dans la conception du rapport. Le conseil consultatif présidé par HTF était composé de représentants du secteurs public et privé du Canada et de la France, tandis que le groupe d'intérêt spécial présidé par le CCIAN était composé de membres partenaires.

Auteurs :

DIACC CCIAN

HUMAN TECHNOLOGY FOUNDATION

Contributeurs :

EY Building a better working world

mccarthy tetrault

DTMV AVOCATS

DIACC CCIAN

Coordinateurs du projet :

Ménehould Michaud de Brisis,
Human Technology Foundation

Joni Brennan,
DIACC

Nous tenons à remercier les représentants du comité consultatif pour leur éclairage et leur soutien lors de l'élaboration du document :

Muriel Barénoud, Director of Civic Engagement, La poste

Colleen Boldon, Director, Digital Lab and Digital ID Programs, Government of New Brunswick

Alexandre Bounouh, CEO, CEA-List

Raphaël de Cormis, VP, Innovation and Digital Transformation, Thales and CEO, Thales Digital Factory

Anne Darche, Corporate Director, Client Experience and Innovation

Anne-Marie Hubert, President of HTF Canadian board and Eastern Canada Managing Partner, EY Canada

Franklin Garrigues, Vice President, External Ecosystems, TD Bank

Ibrahim Gedeon CTO, TELUS

Suzanne Gouin, President, Canada Revenue Agency

Jonathan Kelly, Sous-ministre adjoint à la transformation numérique gouvernementale, Province of Quebec

Mathieu Desrosiers, VP Digital identity and Open banking, Desjardins

Charles Morgan, Partner, McCarthy Tétrault

Jen Mossop-Scott, Associate Partner, EY

Behnaz Saboonchi, Partner, EY-Parthenon

Amar Sharma, Senior Manager, EY

Grimaud Valat, Partner, DTMV

Nous tenons à remercier les organisations suivantes qui ont participé à un groupe d'intérêt spécial et contribué à l'élaboration du document :

CGI

Desjardins

dHub Group

EY

Global Privacy Rights (Formerly OpenConsent)

Human Technology Foundation

McCarthy Tétrault

Onfido

TELUS

The AML Shop

Scotiabank

À propos du CCIAN

Fruit des recommandations du groupe de travail du gouvernement fédéral chargé d'examiner le système de paiements, le Conseil canadien de l'identification et de l'authentification numériques (CCIAN) est une coalition à but non lucratif de chefs de file des secteurs public et privé qui se sont engagés à développer des recherches et des outils pour permettre l'élaboration de solutions et de services canadiens d'identification numérique robustes et évolutifs. Avec la confidentialité, la sécurité et le choix au premier plan de toutes les initiatives du CCIAN, le CCIAN vise à permettre à tous les Canadiens de participer en toute sécurité et en toute confiance à l'économie numérique mondiale.

À propos des groupes d'intérêt particulier du CCIAN

Les groupes d'intérêt particulier (GIP) du CCIAN fournissent un mécanisme pour amener notre communauté de parties prenantes à discuter d'un intérêt spécifique. Ils permettent de mettre en contact des experts du monde entier et d'élargir les conversations en dehors du cercle de membres du CCIAN.

Un GIP du CCIAN ne crée pas de propriété intellectuelle; il se penche plutôt sur une question spécifique pour recommander les étapes suivantes à intégrer dans la stratégie et la feuille de route du CCIAN.

A propos de la Human Technology Foundation

Créée en 2012, HTF est un réseau de plusieurs milliers de membres qui opère à Paris, Montréal, Rome, Bruxelles et Genève dont le but est de contribuer au développement de technologies au bénéfice de l'humain et de remettre la technologie au cœur des débats sociétaux. La mission de la HTF est de coordonner des travaux de recherche multidisciplinaires internationaux et de servir d'interface entre les mondes académique, économique et la société civile. Pour les membres de la HTF, la technologie doit faire partie des solutions pour construire une société plus respectueuse de chacun.

EY | Travailler ensemble pour un monde meilleur

La raison d'être d'EY est de bâtir un monde meilleur, de créer de la valeur à long terme pour les clients, les gens et la société, et de renforcer la confiance à l'égard des marchés financiers.

S'appuyant sur les données et la technologie, les équipes diversifiées d'EY présentes dans plus de 150 pays instaurent la confiance au moyen de la certification, et aident les clients à prospérer, à se transformer et à exercer leurs activités.

Que ce soit dans les services de certification, de consultation, de stratégie, de fiscalité ou de transactions, ou encore, au sein des services juridiques, les équipes d'EY posent de meilleures questions pour trouver de nouvelles réponses aux enjeux complexes du monde d'aujourd'hui.

EY désigne l'organisation mondiale des sociétés membres d'Ernst & Young Global Limited, lesquelles sont toutes des entités juridiques distinctes, et peut désigner une ou plusieurs de ces sociétés membres. Ernst & Young Global Limited, société à responsabilité limitée par garanties du Royaume-Uni, ne fournit aucun service aux clients. Des renseignements sur la façon dont EY collecte et utilise les données à caractère personnel ainsi qu'une description des droits individuels conférés par la réglementation en matière de protection des données sont disponibles sur le site ey.com/fr_ca/privacy-statement. Les sociétés membres d'EY ne pratiquent pas le droit là où la loi l'interdit. Pour en savoir davantage sur notre organisation, visitez le site ey.com.

McCarthy Tétrault

McCarthy Tétrault est l'un des principaux cabinets d'avocats du Canada et propose des solutions juridiques et commerciales stratégiques et novatrices à ses clients, au Canada et ailleurs dans le monde.

Nos juristes travaillent harmonieusement dans tous les domaines de pratique et toutes les régions à partir de nos divers bureaux situés dans les principaux centres d'affaires du Canada, ainsi qu'à New York et à Londres. Nous offrons une prestation de service dans le domaine du droit des affaires, du litige, de la fiscalité, de l'immobilier et du travail et de l'emploi. Nous travaillons également avec tous les paliers de gouvernement pour élaborer des lois et des règlements qui façonnent le marché canadien dans les secteurs industriels constituant le moteur de l'économie canadienne et mondiale.

En offrant à nos clients des solutions et des services novateurs, nous sommes à l'avant-garde du progrès dans la profession juridique, nous créons une valeur ajoutée pour les clients grâce à notre gestion de projet personnalisée, et offrons des solutions de dotation en personnel créatives et des méthodes de tarification alternatives. Notre section primée MT>Divisions, qui regroupe divers secteurs d'activité complémentaires, soutient les clients en leur offrant des solutions novatrices à lancement rapide adaptées pour les clients en utilisant des ressources professionnelles, technologiques, de données ou autres sur demande.

DTMV

DTMV est un cabinet d'avocat français spécialisé en propriété intellectuelle, créé en 1984.

Depuis, son histoire combinée à l'expérience et aux relations fortes entre ses associés appartenant à plusieurs générations ont abouti à la pérennisation d'une vision commune et d'une passion pour le métier d'avocat, qui ont permis une croissance tant de l'équipe que des domaines d'expertise, tel que, notamment, le droit du numérique.

L'expertise de DTMV est reconnue par les principaux guides français et internationaux, tels que Best Lawyers, Chambers, IP Stars, Juve Patent et Leaders League. »

DIACC CCIAN

HUMAN TECHNOLOGY
FOUNDATION